Table des matières

Index des tableaux

Index des figures

Liste des abréviations

POC	« Proof-of-Concept » ou implémentation simple prouvant le fonctionnement d'un système
CEO	Directeur général ou chef de direction d'une entreprise
SGBD	Système de gestion de base de données
SGBD-R	Système de gestion de base de données relationnelle
kWh	kilo Watt heure

Résumé

Le secteur énergétique mondial est aujourd'hui en pleine transformation. Les problématiques soulevées par le réchauffement climatique et la dégradation environnementale, causée par l'exploitation des énergies « fossiles », posent un problème crucial pour la sauvegarde de notre planète. En effet, à l'heure où l'énergie n'est pas encore accessible à tous, les impacts environnementaux découlant de sa production alertent déjà les autorités du monde entier. Dans ce contexte, le Parlement européen et la Confédération helvétique ont tous deux mis en place des stratégies énergétiques visant à réduire l'émission de gaz à effet de serre en substituant les modes de consommation basés sur les énergies « fossiles » par des sources d'énergie dîtes « renouvelables ». Ces sources renouvelables, qui se basent principalement sur la production naturelle d'énergie (vent, soleil, eau, etc.), semblent être l'avenir de la production énergétique mondiale. Cependant, les défis qui découlent de l'adoption de ces nouveaux modèles engendrent à leurs tours de nouveaux défis pour le secteur énergétique.

Notre étude a pour principal objectif d'analyser l'impact de la technologie « Blockchain » au sein d'un système d'information orienté vers l'échange de « kWh » entre des bornes de rechargement. Nous devons être en mesure de comprendre le fonctionnement et les enjeux de cette technologie dans le cadre de la mobilité électrique, et plus largement du secteur énergétique dans son ensemble. Pour ce faire, notre étude présentera trois phases bien distinctes qui viendront répondre aux questions de recherche définie. La première phase se concentre essentiellement sur l'analyse et la compréhension des concepts fondamentaux liées à la technologie « blockchain ». Nous chercherons à comprendre dans le détail son fonctionnement et synthétiser les avantages et inconvénients de la technologie de manière globale. Nous clôturerons cette partie par une analyse des différentes solutions ou implémentations existantes de la « blockchain » au sein du secteur énergétique suisse afin de confirmer la pertinence de notre étude et de constater l'engouement de ce secteur pour cette technologie prometteuse. Lors de la deuxième phase de notre étude, nous présenterons le système « Proof-of-Concept » qui sera implémenté afin de démontrer la pertinence de la technologie dans le contexte de la mobilité électrique. Afin d'être en mesure d'implémenter un tel système, nous devrons être en mesure de sélectionner une plateforme qui soit en adéquation avec les besoins de notre système. Pour ce faire, nous mettrons en place un protocole de sélection qui tiendra compte des principaux facteurs de réussite d'une implémentation « blockchain ». Ce protocole de sélection sera appliqué à un panel de plateformes actuelles afin de sélectionner la solution retenue dans le cadre de note « Proof-of-Concept ». Finalement, nous présenterons les résultats obtenus dans le cadre de cette implémentation afin de valider la pertinence du système.

La mise en place de notre système et les analyses effectuées au sein de l'étude nous permettront d'approfondir et d'identifier les impacts de cette technologie dans le contexte de la mobilité électrique, mais également dans le secteur énergétique dans son ensemble. Nous clôturerons cette étude par la formulation de recommandations exploitables par les acteurs du marché, afin qu'ils puissent rapidement identifier les opportunités et les risques liés à l'avènement de la technologie « blockchain » au sein de ce secteur.

1 Introduction

1.1 Avant-propos

Les challenges auxquels les secteurs de l'énergie doivent faire face aujourd'hui sont nombreux et complexes. En effet, le secteur énergétique mondial est aujourd'hui en pleine transformation et doit affronter des urgences d'ordre climatique, géographique et géopolitiques importantes. L'énergie est devenue une composante essentielle et centrale dans le monde moderne, qui impacte directement notre quotidien et la qualité de vie dont nous bénéficions tous. Aujourd'hui, il est inconcevable d'imaginer notre société sans l'accès à cette énergie, qui conditionne directement notre confort personnel, notre environnement de travail, la qualité des soins dont nous bénéficions, notre alimentation, nos divertissements, notre sécurité et pratiquement toutes les activités auxquelles nous participons quotidiennement (Plain, 2019). Tous ces avantages de notre société moderne ont notamment été obtenus au travers des différentes révolutions industrielles, qui ont profondément bouleversé le mode de fonctionnement de notre société moderne. Nous pouvons notamment citer les trois premières révolutions industrielles, qui sont intimement liées à l'avènement du concept « énergie » au sein de notre société et de nos industries (Zhou et al., 2015).

Tableau 1: Description des trois révolutions industrielles amenées par l'énergie (Zhou et al., 2015)

Nom	Description
Industrie 1.0	L'apparition des premières machines à vapeur (énergie thermique transformée en énergie mécanique) en 1784 a profondément bouleversé le fonctionnement de l'industrie. Les manufactures ont transformé leurs modes de fonctionnement traditionnel et artisanal par les premières machines mécaniques.
Industrie 2.0	Aux alentours des années 1850, l'avènement de l'électricité au sein des industries de l'époque a permis aux entreprises de créer les premières lignes de production, augmentant ainsi grandement les cadences et donnant naissance à la production de masse de produits identiques.
Industrie 3.0	La troisième révolution industrielle sonne l'arrivée de l'électronique et de l'informatique au sein des industries. Cette arrivée provoquera la naissance des premiers automates programmables en 1969. C'est le début de l'automatisation des processus.

Les révolutions industrielles traversées par notre société nous ont permis d'atteindre un niveau de développement qui augmente sans aucun doute notre qualité et notre espérance de vie. Toutefois, il est important de noter que ces succès obtenus, d'un point de vue technologique et sociétal, ont bien souvent été réalisés au détriment de la préservation de notre environnement et de notre climat naturel. En effet, le développement de notre modèle énergétique a historiquement été possible grâce à l'exploitation des énergies dites « fossiles ». Le dictionnaire « Larousse » définit les énergies fossiles de la manière suivante :

> *« Les énergies fossiles font partie des énergies non renouvelables... Les principales sources d'énergies fossiles sont le charbon, le pétrole et le gaz naturel… Elles sont présentes en quantité limitée et ne sont pas renouvelables à l'échelle de temps humaine (leur formation nécessite des dizaines de millions d'années). Leur consommation intensive soulève deux problèmes majeurs pour les sociétés : une crise énergétique liée à l'épuisement des gisements, et une crise climatique liée au dégagement excessif de gaz à effet de serre produits par leur combustion* (Encyclopédie Larousse, 2019). *»*

Au-delà de leur identification (charbon, pétrole, gaz naturel, etc.), le dictionnaire cite d'ambler les problématiques majeures liées à l'utilisation de ce type d'énergie : *l'épuisement des ressources (car limitées) et l'émission de gaz à effet de serre (principalement le « dioxyde de carbone (CO_2) ») inhérent à leur combustion*. Pour comprendre les enjeux liés à cette émission de gaz à effet de serre, le « Global Carbon Project » a créé une carte du monde interactive, permettant de visionner les émissions de CO_2 par pays (Global Carbon Project, 2018).

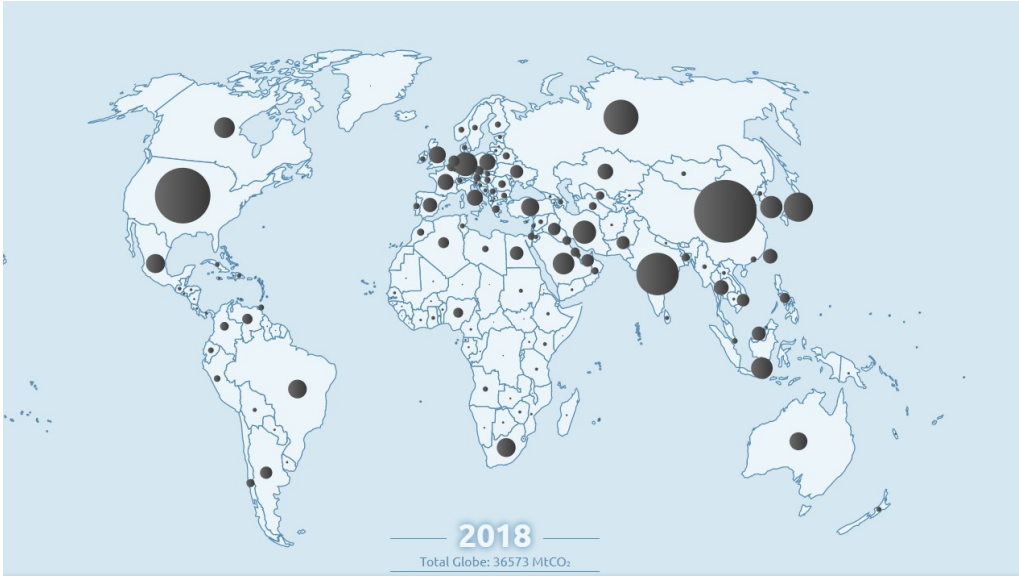


Figure 1: Émissions de CO_2 par pays (Global Carbon Project, 2018)

Nous pouvons constater que les principaux pays émetteurs de gaz à effet de serre sont les pays situés dans l'hémisphère nord de la planète. Sans nécessiter d'avoir recours à une analyse approfondie, nous pouvons d'ores et déjà constater que ces émissions ne sont pas uniquement dues à la superficie du pays ou aux nombres d'habitants. À titre de comparaison, l'Allemagne est actuellement le 6ème producteur de CO_2 mondial pour environ 82 millions d'habitants lorsque le Brésil se situe à la 14ème place avec environ 210 millions d'habitants (Global Carbon Project, 2018). Les chiffres nous permettent de déceler que les plus grands émetteurs de CO_2 de planète sont en réalité les pays les plus développés ou en voient de développement. Nous retrouvons également des pays ayant construit leurs économies autour de l'extraction pétrolière, telles que l'Iran ou l'Arabie saoudite. Les pays ou continents n'ayant pas encore eu droit aux avancées industrielles de notre ère se trouvent être, quant à eux, les pays qui émettant le moins de CO_2 (nous pouvons notamment cité le continent africain). À l'heure où les autorités mondiales alertent la population concernant les effets dévastateurs du réchauffement climatique (majoritairement causé par les gaz à effet de serre), les pays moins développés et n'ayant pas encore bénéficié des avancées offertes par l'accès à l'énergie revendiquent leurs droits de se développer. Cependant, si la revendication et légitime, la reproduction des erreurs passées et l'utilisation d'énergies fossiles pour accélérer leurs développements pourrait avoir des conséquences catastrophiques pour la planète (Fondation d'entreprise ALCEN pour la Connaissance des énergies, 2019). Le secteur énergétique est donc dans l'urgence et doit trouver des alternatives efficientes à l'utilisation des énergies fossiles pour le développement de ces pays à large échelle. Ce processus, également appelé la « décarbonatation énergétique » semble être l'un des défis majeurs du secteur énergétique. En ce sens, le Parlement européen a fait de la lutte contre le réchauffement climatique l'une de ses priorités pour les années futures. Pour y parvenir, il a formulé un cadre législatif et fixé des objectifs à atteindre à courts et moyens

termes. Les propositions amenées par le parlement se déclinent notamment en trois axes majeurs (Parlement européen, 2018).

Tableau 2: Axes de développent adopté par le parlement européen (Parlement européen, 2018)

Axes de développement	Objectifs
Les énergies renouvelables	Augmenter drastiquement la part d'énergie consommée à partir de sources renouvelables (27 % de la consommation globale d'ici 2030)
L'efficience dans la consommation	Améliorer l'efficience de la consommation afin de réduire les émissions de CO_2 et les dépenses inutiles (augmentation de l'efficience de 32.5 % d'ici 2030). Les mesures principales concernent notamment la consommation énergétique des bâtiments, qui représentent 40 % de l'énergie totale consommée en Europe.
Mécanismes de contrôles	Mise en place de métriques et d'organes de contrôle de la suivie des objectifs

Dans une ère où le secteur énergétique souhaite se tourner vers des sources d'énergies renouvelables telles que le soleil ; le vent ou l'eau (Schweiz, 2020), les défis qui découlent de cette volonté restent néanmoins nombreux. En adéquation avec cette stratégie, le pourcentage de véhicules électriques en Suisse a augmenté de 432 % lors des cinq dernières années (Droz, 2019). Ce chiffre démontre l'engouement croissant de la part de la population vis-à-vis des moyens de locomotions énergétiquement « propres ». Selon une récente étude menée par le « BCG[1] », le nombre de ventes de véhicules électriques pourrait dépasser celui des véhicules thermiques dès 2030 (Boston Consulting Group, 2020). Si ces prévisions annoncent des répercussions positives pour notre environnement, il est également révélateur de la charge attendue en matière de consommation électrique lors des années à venir. Pour faciliter cette transition et répondre au besoin énergétique de la population, le secteur devra se tourner vers de nouveaux modèles de production/consommation capables d'absorber cette charge, tout en restant « écoresponsable » vis-à-vis de l'environnement.

1.2 Contexte

Cette étude a été rédigé dans le cadre d'une thèse de Master, suivi au sein du Master of Science HES-SO en Business Administration, orienté « Management des Systèmes d'information » à Lausanne en Suisse. Elle vise à valider les compétences acquises lors du cursus en élaborant un travail de recherche approfondie sur une thématique ayant un lien avec la gestion des systèmes d'information. Ce travail a été effectué dans les limites des cadres imposés par le projet. Il est donc soumis à des limitations, tant en termes de volume (nombre de pages) que de temps (délai du rendu). Le projet a été réalisé de manière individuelle et supervisé par le Professeur David Wannier, enseignant au sein de la formation « HES-SO » Master à Lausanne et au Valais.

La thématique abordée par notre étude s'inscrit dans un projet initié par le « SCCER - FURIES » qui représente « *le centre national de compétences axé sur la mise à niveau de l'infrastructure électrique suisse. Il répond aux défis liés au réseau électrique soulevés par l'ES2050, en fournissant aux gestionnaires de réseau des outils de planification, de surveillance et d'exploitation améliorés par l'intelligence* » (SCCER-FURIES, 2020b). Le projet intervient dans le contexte de la « Swiss Energy Strategy 2050 (ES2050) », qui cherche à réduire l'impact environnemental de la production énergétique suisse (SFOE, 2018). Le « SCCER - FURIES » préconise notamment un certain nombre de mesures clés, nécessaires au maintien de la stabilité du réseau électrique suisse.

1 BCG : Boston Consulting Group

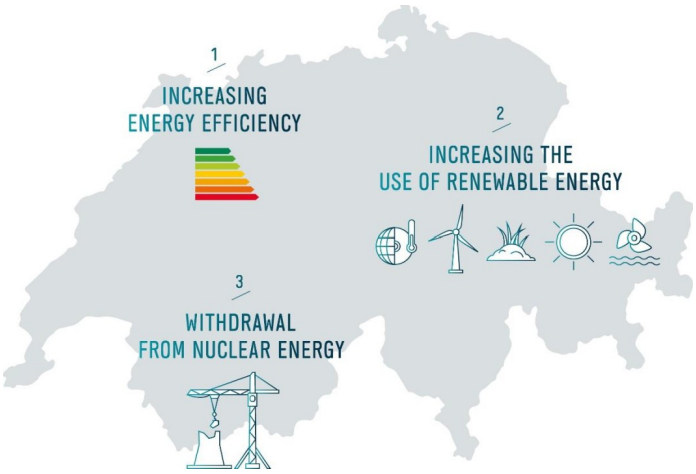


Figure 2: Les trois mesures nécessaires à la stabilité du réseau électrique suisse (SCCER-FURIES, 2020a)

Notre étude fait suite à une première thèse de Master articulé au tour de la même thématique et intitulé « EV Blockchain Charging : Système de facturation autonome pour recharge des voitures électriques basé sur la blockchain » (Vianin, 2018).

1.3 Objectifs

Notre étude a pour principal objectif d'analyser l'impact de la technologie « Blockchain » au sein d'un système d'information orienté vers l'échange de « kWh » entre des bornes de rechargement. Nous devons être en mesure de comprendre le fonctionnement et les enjeux de cette technologie dans le cadre de la mobilité électrique, et plus largement du secteur énergétique dans son ensemble. Une implémentation « Proof-of-Concept » est attendue pour démontrer la faisabilité du système. Pour y parvenir, nous avons défini la question de recherche principale suivante :

> *Quels sont les impacts et enjeux de la technologie "blockchain" dans le contexte de la mobilité électrique ?*

Pour tenter de répondre à cette question, nous avons subdivisé la problématique en quatre questions de recherches secondaires qui nous permettront de répondre aux différents aspects soulevés par la question principale :

- *RQ1* : Qu'est-ce que la « blockchain » et quels en sont les concepts fondamentaux ?
- *RQ2* : Qu'elles sont les exemples et solutions existantes sur le marché, dans le contexte de la mobilité électrique ?
- *RQ3* : Quels sont les critères d'évaluation pertinents à la sélection d'une solution « blockchain » ?
- *RQ4* : Quels sont les apports d'un système basé sur la « blockchain » par rapport à un système d'information traditionnel, dans le contexte de la mobilité électrique ?

Nous allons maintenant présenter la méthodologie mise en place pour la réalisation de ce travail afin de comprendre les enjeux liés à la technologie « blockchain » au sein du secteur énergétique, et plus particulièrement celui de la mobilité électrique.

2 Méthodologie

Nous allons construire notre étude au tour de trois phases principales, toutes visant à répondre aux questions de recherches que nous avons identifiées en introduction de ce travail. Lors de la première phase, nous allons explorer les concepts fondamentaux de la technologie « blockchain » afin d'être en mesure de comprendre le fonctionnement et les enjeux liés à ce concept. Cette exploration sera faite par l'intermédiaire du chapitre « Revue de la littérature », durant lequel nous tenterons d'exposer l'état de l'art en matière de technologie « blockchain ». Lors de cette partie, nous ferons également le lien entre la technologie et les exemples existants sur le marché, notamment dans le cadre de la mobilité électrique, afin confirmer le potentiel de la « blockchain » au sein de ces secteurs d'activités. En clôture de cette phase, nous devrions avoir répondu aux questions de recherche *RQ1* et *RQ2*.

La deuxième phase de l'étude s'appuiera sur les connaissances acquises lors de la phase précédente afin de prototyper l'implémentation que nous devons réaliser dans le cadre de ce travail. Nous détaillerons l'architecture et les interactions de notre système afin d'illustrer la pertinence de la technologie et la faisabilité du projet. L'élaboration du système à implémenter nous conduira vers la sélection d'une plateforme « blockchain » pertinente dans le cadre de notre travail. Pour réaliser ce choix, nous devrons analyser les critères de sélection pertinents au choix d'une technologie qui soit en adéquation avec les besoins de notre système. Nous approfondirons donc ces concepts afin de mettre en place un processus de sélection cohérent, qui tient compte des spécificités de l'environnement dans lequel évoluera la technologie. Le résultat de l'élaboration de ce processus sera le choix d'une plateforme « blockchain », que nous utiliserons comme socle de notre « POC ». De plus, il répondra de manière directe à notre question de recherche *RQ3*. Nous finaliserons cette phase par la présentation du système mis en place et des résultats obtenus dans le cadre de cette étude.

La troisième et dernière phase de ce travail aura pour objectif d'analyser et synthétiser les résultats obtenus lors de nos analyses et développements, afin de les mettre en perspective avec le secteur énergétique. Les compétences acquises vis-à-vis de la technologie « blockchain », lors de la phase développement, nous permettrons d'en analyser la pertinence et les impacts au sein de son environnement. Nous conclurons cette étude par une synthèse des résultats obtenus et par l'analyse des axes de développements possibles ou non abordés lors de ce travail.

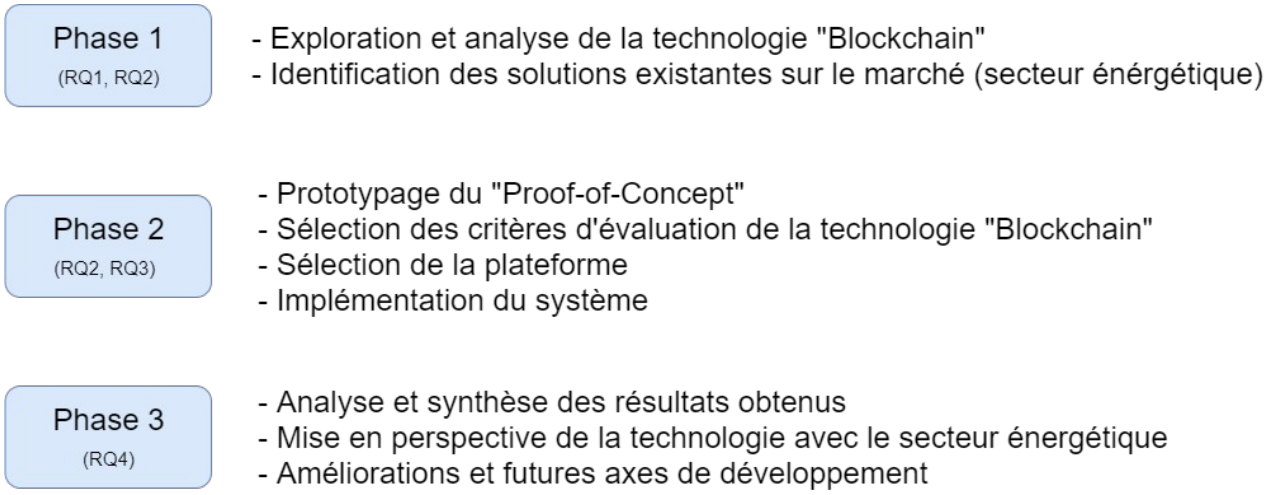


Figure 3: Les trois phases de construction de l'étude

3 Revue de la littérature

La revue de la littérature a pour objectif de définir et approfondir les concepts fondamentaux abordés lors de ce travail. Nous allons décomposer notre revue de la littérature en deux parties distinctes afin d'en accroître la lisibilité et de clairement répondre à nos deux premières questions de recherche :

1. Qu'est-ce que la « blockchain » et quels en sont les concepts fondamentaux (RQ1)
2. Quelles sont les solutions existantes sur le marché dans le contexte de la mobilité électrique (RQ2)

La section suivante va donc s'intéresser à l'approfondissement des concepts fondamentaux porté par la technologie « blockchain » afin de répondre à notre première question de recherche.

3.1 Introduction à la « Blockchain »

La technologie « Blockchain » fait partie intégrante du panorama des technologies à suivre dans le monde des sciences et des technologies de l'information. Elle a émergé aux yeux du grand public en 2008 avec l'avènement du « Bitcoin » qui, quelques années plus tard, créa un réel séisme au sein des places financières. En effet, le 16 décembre 2017, la valeur d'un bitcoin atteignait la valeur record de 19'346.44 dollars (Bitcoin.com, 2020). L'émergence et le succès de cette nouvelle cryptomonnaie ont, par transitivité, mis en lumière la technologie qui la supporte : *la blockchain*. L'entreprise « Gartner » a identifié la blockchain comme faisant partie des dix technologies « stratégiques » pour les entreprises en 2020 (elle occupait également le classement en 2017, 2018 et 2019)(Panetta, 2019b). Ce classement énumère les technologies et concepts ayant un impact fort sur les enjeux rencontrés par les entreprises dans leurs domaines respectifs. Ainsi, la blockchain est reconnue comme étant une technologie ayant la capacité d'impacter les entreprises, tant sur leurs structures et organisations que sur les services qu'elles proposent. Le magazine « computerworld » estime même que 2020 sera l'année de la maturité pour cette technologie, durant laquelle nous verrons la blockchain appliquée dans des domaines pertinents, au détriment des implémentations diverses et variées auxquelles nous assistons aujourd'hui (Davidson, 2020). Cette volonté de vouloir massivement appliquer la technologie blockchain peut être illustrée par la célèbre courbe « Gartner Hype Cycle for Emerging Technologies », publiée une fois par an par la société américaine. La courbe illustre l'émergence des nouvelles technologies qui devraient être au cœur des préoccupations des entreprises lors des prochaines années (Panetta, 2018).

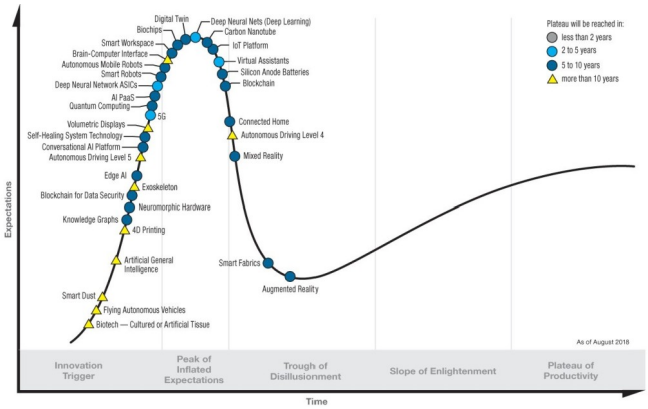


Figure 4: Courbe "Gartner Hype Cycle for Emerging Technologies 2018"

Cette courbe tente de classifier la maturité des technologies en partant du postulat qu'elles devront traverser cinq phases bien distinctes pour atteindre leurs piques de maturité. La première phase est celle du « déclenchement de l'innovation » et représente donc la technologie dans sa genèse. À ce stade, la technologie suscite l'intérêt des acteurs et va aboutir à des analyses sur ses capacités ainsi qu'à l'implémentation de divers « Proof-of-concept (POC)[2]». Les résultats obtenus lors de cette phase conduiront naturellement la technologie à la deuxième étape, à savoir le « pic d'attentes démesurées ». Lors de cette phase, les attentes liées à la technologie sont à leurs paroxysmes, car l'euphorie et le manque de maîtrise vis-à-vis de la technologie poussent les acteurs à en voir que les aspects « positifs ». De ce fait, cette phase conduit les acteurs à investir dans des projets liés à la technologie, sans la maîtrise et l'expérience nécessaires. Les premiers résultats obtenus suite à ces implémentations font basculer la technologie dans la troisième phase, « le creux de la désillusion ». Une fois le projet lancé, les premières difficultés vont apparaître, qu'elles soient liées à la technologie ou à sa mauvaise application. Cette étape va généralement susciter un sentiment de déception ou de réticence vis-à-vis de la technologie. Néanmoins, les acteurs vont analyser les raisons liées à cet échec et en tirer des analyses concernant la bonne utilisation de la technologie. Ainsi, la montée en compétences et l'expérience acquise vis-à-vis de la technologie, lors des différents projets, vont faire transiter cette dernière vers la quatrième phase, « la pente de l'illumination ». Lors de cette période, les acteurs prennent conscience des erreurs commises et prennent du recul quant aux possibilités offertes par cette dernière. Ainsi, ils utilisent leurs propres expériences et celles des autres acteurs pour cibler plus précisément leurs besoins vis-à-vis de la technologie. Finalement, lorsque ce niveau de connaissance a été atteint, la technologie peut être considérée comme étant mature et rejoint la dernière phase de la courbe, «le plateau de la productivité».

En 2018, nous pouvons constater que la technologie «blockchain» apparaît comme étant à l'entrée de la phase du «creux de la désillusion». Cela indique que la technologie a en effet été massivement utilisée par les acteurs et que les premiers résultats obtenus ne sont pas toujours à la hauteur des attentes. Depuis son apparition, la blockchain a suscité la curiosité et un vif intérêt de la part d'un ensemble très varié de secteurs d'activités. En effet, le potentiel de cette technologie a rapidement été perçu comme étant une réponse à de nombreux problèmes rencontrés dans l'industrie, dans les administrations publiques (Pignon, 2017), dans l'agroalimentaire (Sharma, 2019b), dans l'audiovisuel (Wessbecher, 2018) et dans bien d'autres domaines. Fort de ce succès, la technologie « blockchain » a fait l'objet de nombreuses tentatives d'implémentations au sein de nouveaux projets ou d'intégrations au sein de systèmes existants. Un récent rapport publié par la «CAICT (China Academy of Information and Communications Technology)» abonde en ce sens. Le rapport estime à 80'000 le nombre de projets lancé dans le monde, en lien avec la blockchain, depuis 2009. Au-delà de l'engouement suscité par la technologie, le rapport fait état d'un fait plus surprenant : *92 % des projets (sur les 80'000) ne seraient aujourd'hui plus maintenus par les équipes de développement ou se seraient soldé par un échec. De plus, la durée de vie moyenne des projets avoisinerait les 15 mois (Maloney, 2018).* Ces statistiques, aussi impressionnantes soient-elles, confirment le positionnement de la technologie au sein de la courbe de «Gartner». Le taux d'échec élevé des projets en lien avec la blockchain confirme que la technologie est encore en phase d'adoption par les acteurs. «Gartner» estime que la technologie atteindra «le plateau de la productivité» d'ici cinq à dix ans. Ces chiffres indiquent clairement que la blockchain est encore en phase d'expérimentation chez la plupart des acteurs et que le niveau de maturité nécessaire à la maîtrise de son écosystème n'est pas encore atteint. Il est donc nécessaire, pour tout nouveau projet en lien avec cette technologie, d'accentuer les phases d'analyses et de conception afin de garantir que les besoins du projet soient en accord avec les prérequis inhérents aux concepts de la blockchain. Si la blockchain ne figure plus dans la courbe des technologies émergentes en 2019 (Panetta, 2019a), son positionnement est confirmé comme étant au plus bas de la phase du « creux de la désillusion » dans une courbe spécifiquement dédiée aux applications de la blockchain dans divers secteurs d'activités (Rimol, 2019) (cette courbe sera présentée ultérieurement dans ce rapport). Il est néanmoins important de préciser que les analyses fournies par cette

2 Proof-of-concept : Implémentations simples, capables de démontrées les capacités et limites d'un système sans avoir à l'implémenter dans un environnement de production.

courbe représentent le niveau de maturité et de maîtrise d'une technologie vis-à-vis des acteurs qui l'exploitent. Elle n'évalue en aucun cas le potentiel ou la pérennité de cette même technologie. De ce fait, la technologie « blockchain » semble avoir traversé les phases les plus fluctuantes de son adoption afin transité vers une phase de stabilité qui garantira une utilisation plus efficiente de son potentiel.

Afin de comprendre et identifier les tenants et les aboutissants de cette technologie, nous allons réaliser une analyse approfondie de son origine et des concepts fondamentaux inhérents à cette dernière. Cette analyse nous permettra de répondre à notre première question de recherche (*RQ1*) et de mettre la technologie en lien avec le monde de l'énergie, et plus particulière celui de la mobilité électrique.

3.1.1 Historique

En préambule de cette revue de la littérature, nous avons mentionné le lien existant entre l'émergence de la fameuse cryptomonnaie « Bitcoin » et celle de la technologie « blockchain ». En effet, la distinction entre les deux entités n'a pas toujours été facile à établir pour les non-initiées. Cependant, il est primordial de distinguer les deux concepts afin d'entrevoir les possibilités offertes par la technologie « blockchain » lorsqu'elle est utilisée dans un autre secteur que celui de la finance, et plus particulièrement en tant que cryptomonnaie.

Le « Bitcoin » est une monnaie virtuelle créée en 2008 par Satoshi Nakamoto[3]. Il est important de différencier l'appellation « Bitcoin », avec un « B » majuscule, de « bitcoin » avec un « b » minuscule. Effectivement, la première fait référence au nom donné à la cryptomonnaie (ex. : euros, francs, dollars, etc.). La deuxième, pour sa part, fait référence « *au nom du protocole décrivant le fonctionnement du réseau sur lequel la monnaie circule. Ce protocole, c'est la Blockchain, où la création monétaire et la validation des transactions s'effectuent de manière horizontale et transparente...* »(Blockchain France Associés, 2016). Nous comprenons donc ici que le protocole « bitcoin » est en réalité la première implémentation publique de la technologie « blockchain », destinée soutenir le fonctionnement d'une monnaie virtuelle, baptisée « Bitcoin » par son auteur. Historiquement, et sur la base de cette implémentation, plusieurs centaines de nouvelles cryptomonnaies ont vu le jour depuis 2008 (le site « CoinMarketCap » répertorie 5'089 cryptomonnaies à ce jour (CoinMarketCap, 2020). Si ce nombre nous donne une indication intéressante sur la diversité du marché, il n'est cependant pas exhaustif). Parmi les monnaies ou plateformes les plus notables, nous pouvons citer « Ethereum (ETH) (Ethereum Foundation, 2020) », « XRP (XRP) (Ripple, Inc., 2020) », « LiteCoin (LTC) (Litecoin Project, 2020) », et bien d'autres. Ces implémentations ont toutes en commun la volonté d'utiliser la technologie « blockchain » afin de créer un nouvel écosystème dédié aux paiements en ligne, et donc des monnaies virtuelles. Néanmoins, le marché a vu émerger de nouvelles implémentations de cette technologie qui ne sont pas directement adressées à ce cas d'utilisation. En effet, le potentiel caché derrière la technologie « blockchain » a poussé l'industrie à analyser les impacts et applications possibles de ce concept à plus large échelle. Pour comprendre la raison de ce questionnement, nous devons étudier les concepts fondamentaux de cette technologie afin d'en identifier les principales caractéristiques et applications possibles.

3.1.2 Concepts fondamentaux

La littérature scientifique et spécialisée regorge d'informations concernant la technologie « blockchain ». « Blockchain France » la définit de la manière suivante :

> *« La Blockchain est une technologie de stockage et de transmission d'informations. Cette technologie possède en particulier trois caractéristiques majeures : elle est transparente, sécurisée, et fonctionne sans organe central de contrôle* (Blockchain France Associés, 2016). »

3 « Satoshi Nakamoto » est un pseudonyme utilisé par le(s) créateur(s) du Bitcoin. Il à été utilisé lors de la publication du document décrivant le fonctionnement du Bitcoin. L'identité réel de ce « personnage » reste à ce jour inconnu.

Si cette définition reste encore aujourd'hui d'actualité (2016), l'évolution de la technologie ces dernières années nous pousse à compléter ce constat. En effet, il n'est pas aisé de formuler une définition unique pour cette technologie qui voit sans cesse son fonctionnement et ses domaines d'applications évoluées. Dans un article publié en mars 2019, « Wattana Viriyasitavat et Danupol Hoonsopon » souligne la même difficulté à qualifier de manière unique la « blockchain », tant elle dépend du contexte dans lequel elle est utilisée. Fort de ce constat, ils la définissent de la manière suivante :

> *« La Blockchain est une technologie qui permet l'immuabilité et l'intégrité des données, dans laquelle un enregistrement des transactions effectuées dans le système est conservé sur plusieurs nœuds distribués qui sont liés dans un réseau peer-to-peer (Viriyasitavat & Hoonsopon, 2019). »*

La définition apportée par « Wattana Viriyasitavat et Danupol Hoonsopon » semble pertinente dans la mesure où elle se concentre sur l'essence même de la technologie. Elle reste suffisamment générique pour ne pas attribuer des superlatifs tels que « transparante » et « sans organe de contrôle central », qui peuvent être sujets à débats selon le type de « blockchain » analysé. Le CEO de l'entreprise « Coin Sciences » abonde en sens en présentant une définition plus accessible et orientée « métier » :

> *« Une blockchain est un nouveau type de base de données qui permet à plusieurs parties prenantes de partager la base de données et de pouvoir la modifier de manière sûre et sécurisée, même si elles ne se font pas confiance (Hileman & Rauchs, 2017). »*

En effet, nous pouvons définir et visualiser la technologie « blockchain » comme étant un nouveau type de base de données « distribuée », permettant de faire circuler des informations au sein d'un réseau décentralisé.

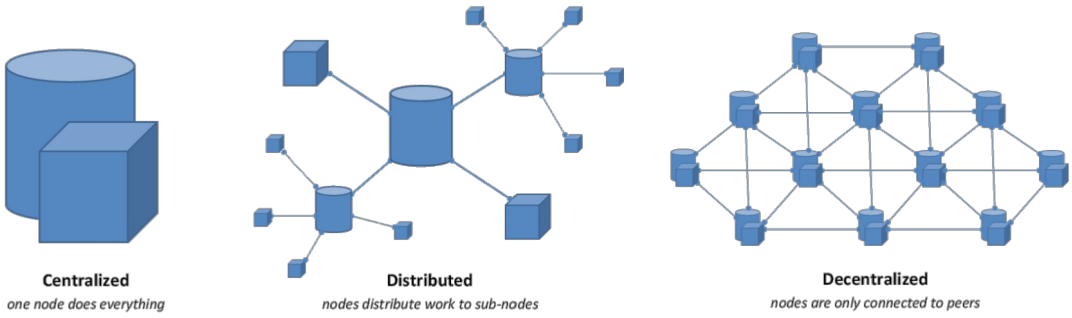


Figure 5: Illustration des termes "centralisé", "décentralisé" et "distribué" (Grange, 2016)

Si les bases de données « distribuées » existaient déjà avant l'avènement de la « blockchain » (ex. : base de données « Oracle (Oracle Corporation, 2002) », « PostgreSQL (PostgreSQL wiki, 2018) », « Microsoft SQL Server (Microsoft Corporation, 2017) »), elle se distingue particulièrement par le fait qu'elle soit « décentralisée » et qu'elle permette de valider les données en instaurant un consensus entre toutes les différentes parties prenantes du réseau (Hileman & Rauchs, 2017). Néanmoins, une fois encore, nous devons nuancer ces informations en fonction du type de « blockchain » analysé. Le terme « décentralisé » est très fréquemment utilisé dans la littérature lorsque l'on parle de la technologie « blockchain ». Cependant, il important de comprendre le contexte dans lequel ce qualificatif est utilisé pour comprendre les réels enjeux liés aux différentes solutions existantes sur le marché. « Vitalik Buterin », le célèbre créateur de la blockchain « Ethereum », a rédigé un article expliquant l'importance de comprendre et nuancer la notion de « décentralisation » au sein de la blockchain. Il identifie trois axes d'analyses possibles lorsque l'on parle d'un système « centralisé » ou « décentraliser » (Buterin, 2017) :

1. *(Dé)centralisation architecturale* : il identifie le nombre de périphériques ou machines (physiques) qui composent le système. L'ensemble du système repose sur une machine physique (centralisé) ou sur plusieurs machines distinctes (décentralisé).
2. *(Dé)centralisation politique* : il identifie le nombre de parties prenantes ou organisations qui contrôle le système. Le système est contrôlé par une seule entité ou entreprise (centralisé), ou par un ensemble d'individus n'ayant aucun lien entre eux (décentralisé).
3. *(Dé)centralisation logique* : il identifie la cohérence ou la logique du système dans son ensemble. Le système, quel que soit son organisation architecturale et politique, garantit une logique métier uniforme pour les utilisateurs (centralisé) ou il applique des règles distinctes en fonction de la configuration de son environnement (décentralisé).

La combinaison de ces critères permettrait de plus facilement comprendre la réelle portée du terme « décentralisé » lorsque l'on souhaite analyser un système ou une technologie telle que la « blockchain ». Sur la base de ces trois axes d'analyses, « Vitalik Buterin » positionne la « blockchain » au sein de la matrice suivante :

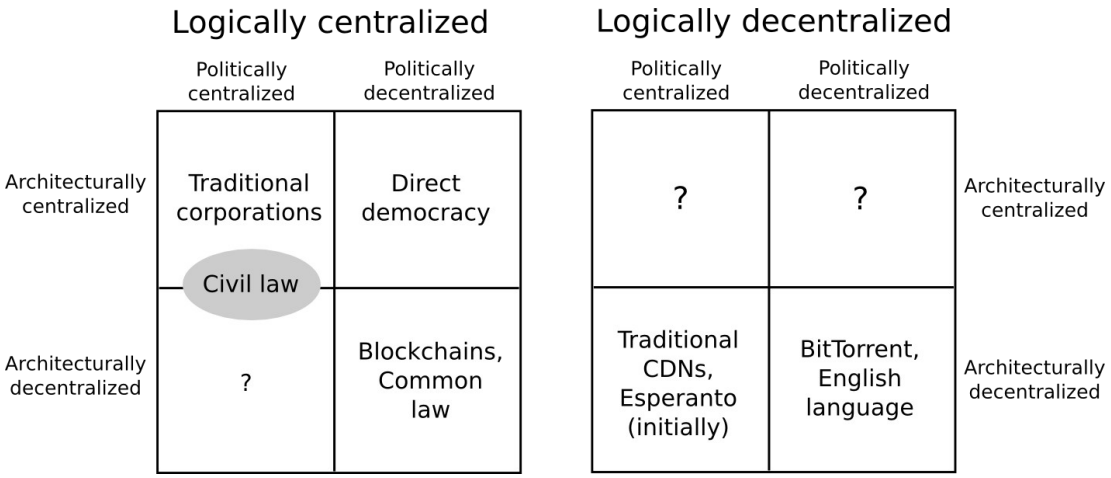


Figure 6: Axes d'analyses possibles pour la "décentralisation" d'un système (Buterin, 2017)

L'analyse faite par « Vitalik Buterin » classifie la « blockchain » comme étant un système politiquement et architecturalement décentralisé. En effet, les premières implémentations de la blockchain (ex : « Bitcoin », « Etheurem ») ont la particularité d'être des blockchains « *publiques* ». Cela signifie que quinconce peut rejoindre le réseau et participer aux transactions au sein de la blockchain. De ce fait, les transactions sont validées et inscrites au sein de la blockchain via un système de « *consensus* » qui est propre à chaque implémentation de la blockchain. Cette autonomie et transparence au sein du système garantit que personne ne peut contrôler ou modifier le fonctionnement du système. De plus, chaque acteur du système dispose d'une copie de la « blockchain » sur sa machine. Nous pouvons ainsi qualifier le système de « distribué » et architecturalement « décentralisé ». Cependant, le fondateur d' « Ethereum » qualifie la blockchain comme étant logiquement centralisé. En effet, quel que soit l'acteur qui interagit avec la blockchain, il sera soumis aux mêmes règles « métier » implémentées par le système. L'analyse de « Vitalik Buterin » est donc parfaitement recevable. Néanmoins, nous nuancerons ce positionnement ultérieurement dans ce rapport, dû à l'avènement d'un nouveau type de blockchain : les blockchains « *privées* ».

Nous allons maintenant explicité le fonctionnement interne d'un système « blockchain » afin de comprendre ses spécificités par rapport un système de base de données traditionnel. En effet, nous avons pu voir que la

« blockchain » est une technologie qui peut s'apparenter à un nouveau type de base donnée, capable de stocker et diffuser des informations au sein d'un réseau distribué et décentralisé. Toutefois, le mode de fonctionnement et la méthode de stockage des données de la blockchain sont bien différents des systèmes traditionnels. Une base de données « classique » (ex. : « Oracle », « PostgreSQL », « Microsoft SQL Server ») repose sur un système de gestion communément appelé « SGBD » ou « SGBD-R ». Si nous n'allons pas expliciter l'ensemble des possibilités de ces systèmes, il est néanmoins important de préciser que ces systèmes stockent et structurent les données dans des entités que l'on appelle communément des « tables ». Chaque « table » dispose d'un certain nombre de « colonnes » qui correspondent à une propriété de la donnée que le souhaite stocker. Par exemple, une table « voiture » pourrait contenir les colonnes « numero », « marque », « nombre_portes » et « couleur ». Une fois cette structure définie au sein du SGBD, le système va stocker des informations dans la « table », que l'on peut nomme comme étant des « enregistrements » ou des « lignes ». Nous obtenons donc une structure semblable au tableau ci-dessous :

Tableau 3: Illustration d'une table "voiture" au sein d'un SGBD

numero	marque	nombre_portes	couleur
1	WW	5	blanc
2	BMW	5	bleu
3	FIAT	3	rouge

La table « voiture » peut contenir autant d'enregistrement que l'on souhaite (selon les règles définies par le SGBD). Il est ensuite possible pour un utilisateur ou administrateur de la base de données d'ajouter, modifier ou supprimer des données au sein de la table (ces actions peuvent être restreintes, journalisées et traquées par le système). En opposition avec ce mode de fonctionnement, la « blockchain » structure et stocke les données différemment, ce qui constitue l'une de ses caractéristiques fondamentales. Dans sa traduction française, le mot « blockchain » signifie littéralement « chaîne de blocs ». Il s'avère que ce nom est particulièrement représentatif du mode de fonctionnement de cette technologie. En effet, contrairement à la structure en « tables » proposées par les SGBD classiques, la blockchain structure et stock l'information sous forme d'une « transaction », qui sera incorporée au sein d'un « bloc », qui à son tour sera ajouté à une chaîne de blocs « immuables ». Agissant comme une véritable « chaîne » physique, les « blocs » s'enchaînent par ordre de création (le premier bloc crée au début de la chaîne et le dernier bloc crée à la fin de la chaîne) et sont liés entre eux par référence (un bloc dispose de la référence du bloc précédent). Ainsi, il est possible de reconstituer l'entièreté de la chaîne en partant du dernier bloc de la chaîne (The Linux Foundation, 2019a).

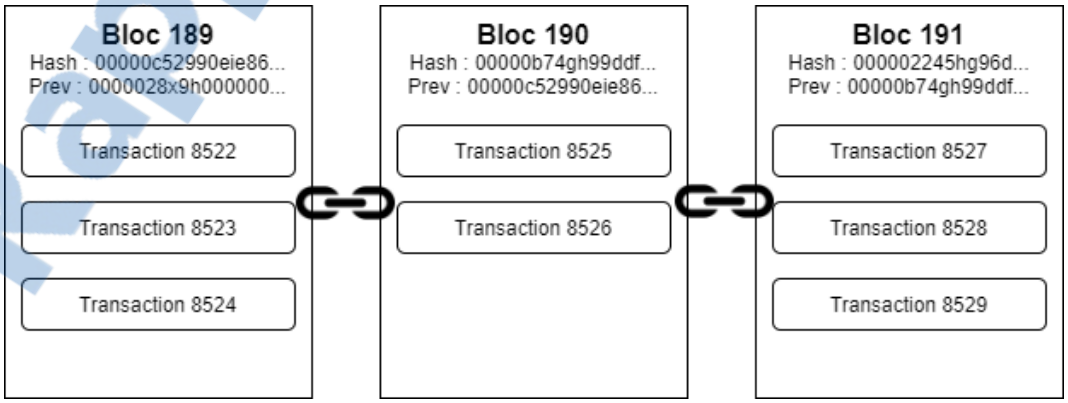


Figure 7: Fonctionnement d'une "chaîne de blocs" traditionnelle

Ce mode de fonctionnement est généralement commun à toutes les implémentations de la blockchain (les informations définissant un bloc peuvent sensiblement varier). Un « bloc » est défini par un numéro et une référence unique (communément appelé « hash »), générée à partir des informations contenues au sein du bloc. Une fonction de hachage cryptographique a pour objectif de générer une valeur (ou emprunte numérique) unique pour un bloc (ou un fichier, un document, etc.) à partir des données qui le compose. Cette approche est fondamentale à la compréhension du système, car elle est la seule garante à l'immuabilité des données et de la chaîne de bloc. L'illustration présentée ci-dessus représente trois blocs, contenant chacun un certain nombre de transactions. Chaque « bloc » dispose de sa propre empreinte numérique (hash) générée à partir des données qu'il contient (valeur « hash » sur l'illustration). Le « bloc » dispose également de l'empreinte numérique (hash) du « bloc » qui le précède (valeur « prev » sur l'illustration). Cette information nous donne une précision importante sur le fonctionnement de la chaîne : *l'empreinte numérique unique d'un bloc (« hash ») est calculée en fonction de données du bloc, y compris le « hash » du bloc précédent.*

Ce comportement est le concept clé qui garantit qu'un « bloc » une fois crée et insérer dans la blockchain ne peut plus être supprimé, ou modifier sans impacter l'ensemble des blocs qui le suivent. Afin d'illustrer ce propos, nous allons simuler une tentative de modification frauduleuse d'un bloc, après sa création et sa validation au sein de la « blockchain ». Considérons l'état de la chaîne présenté ci-dessus (Figure 7) comme étant un état sain et valide. Étant dans un environnement distribué et décentralisé, un utilisateur du réseau à la possibilité de tenter de modifier sa version « locale » de la blockchain. Pour ce faire, il tente d'ajouter une transaction frauduleuse au sein du « bloc » numéro 190. Une fois qu'il aura validé cette transaction au sein de sa copie « locale », le système va automatiquement recalculer la valeur « hash » du bloc numéro 190. Les données ayant changé, l'empreinte générée par la fonction de hachage ne sera désormais plus identique à celle de la version précédente.

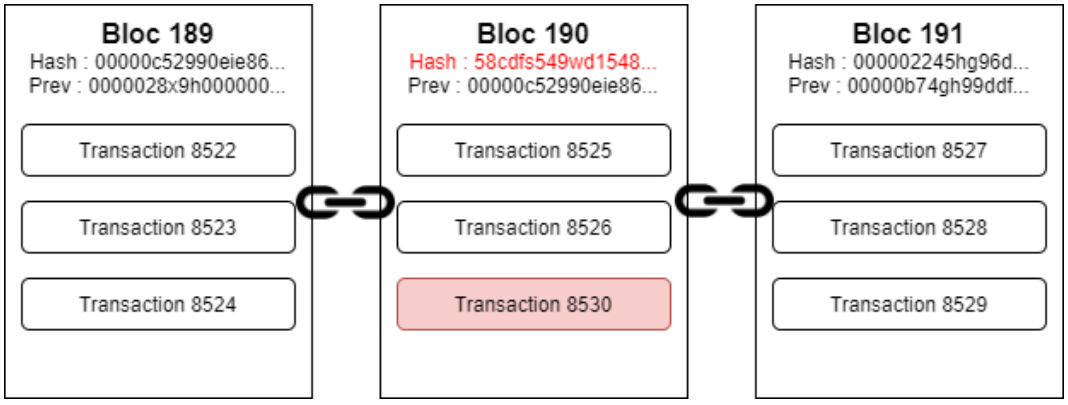


Figure 8: Tentative frauduleuse de modifier un bloc dans la chaîne

La modification de l'empreinte numérique (« hash ») du « bloc » numéro 190 va inévitablement créer une cassure dans le référencement du bloc suivant. En effet, le « bloc » 191 n'est maintenant plus en mesure de trouver la signature numérique de son prédécesseur et va donc devoir la mettre à jour pour maintenir la chaîne intacte. Cependant, la modification de la référence vers le « bloc » 190 va engendrer une mise à jour de son état, et donc générer une nouvelle empreinte numérique (« hash ») pour le « bloc » 191. De ce fait, les données n'étant plus les mêmes qu'à l'état précédent, sa valeur va également être modifiée. Ce changement d'empreinte au sein du « bloc » numéro 191 va à son tour engendrer une cassure pour le « bloc » 192. Cette réaction en chaîne va se poursuivre jusqu'à ce que tous les « blocs », en partant du bloc corrompu (bloc numéro 190), soient mis à jour avec leurs nouvelles empreintes numériques (« hash »).

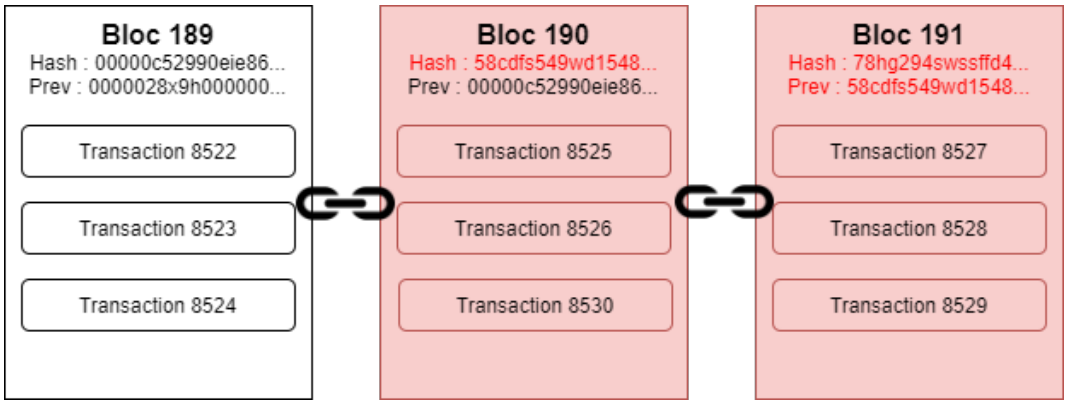


Figure 9: État de la chaîne après la modification frauduleuse

Après avoir modifié le « bloc » numéro 190, tous les blocs qui le suivent auront donc inévitablement changé de signature. Lorsque l'utilisateur va transmettre « sa » version de la blockchain au reste des utilisateurs du réseau, un conflit va naître entre la version de la chaîne détenue par l'ensemble des participants et celle proposée par l'utilisateur malveillant. Pour pallier à cette éventualité, la blockchain implémente un système capable d'arbitrer une telle situation ainsi que de valider ou rejeter une version de la chaîne proposée par un utilisateur. Ce système est communément appelé le « *consensus* ». Il existe divers mécanismes de « consensus » développés spécifiquement pour les implémentations blockchain. Nous détaillerons certains d'entre eux lors de la partie « Analyses et développement » de ce rapport. Pour notre illustration, il est nécessaire de comprendre que ce système de « consensus » va demander à une partie ou à l'ensemble des participants du réseau de vérifier la véracité de la chaîne soumise. Le résultat obtenu par les participants chargé de la vérification va valider ou rejeter le nouvel état de la chaîne. Si la chaîne est rejetée, l'état de la chaîne ne sera pas mis à jour. Dans l'autre éventualité, tous les participants du réseau mettront à jour leur version « locale » avec le nouvel état de la chaîne (Zheng et al., 2017).

Par l'intermédiaire de la démonstration réalisée ci-dessus, nous avons abordé et explicité les cinq composants indispensables à la compréhension d'un système « blockchain », en accord avec le rapport publié par « Garrick Hileman et Michel Rauchs » (Hileman & Rauchs, 2017), qui sont :

1. ***La cryptographie*** : la « blockchain » utilise un grand nombre de techniques « cryptographiques » afin de garantir l'immuabilité des blocs. Nous avons abordé les fonctions de hachage utilisé pour la génération de l'empreinte numérique des blocs. Cependant, il est important de savoir que d'autres techniques de cryptographie sont également utilisées par la blockchain pour assurer son fonctionnement. Nous pouvons notamment citer « l'arbre de merkle » qui est un élément essentiel et qui permet aux mécanismes de « consensus » d'accélérer la vérification des blocs et de leurs transactions (De Quénetain, 2018). La cryptographie est également utilisée au sein des blockchain « publiques » afin d'identifier de manière unique les participants du réseau. Cette identification se fait via le mécanisme de clés « publiques/privées » (Pleynet, 2017).
2. ***La distribution et la décentralisation du système*** : la « blockchain » est considérée comme étant un système « distribué » et « décentralisé ». Ces caractéristiques font de la « blockchain » un système « autonome », ne nécessitant pas de tiers de confiance pour gérer son état (position nuancée dans le cadre des blockchains « privées »).
3. ***Le mécanisme de « consensus »*** : la « blockchain » dispose d'un mécanisme capable de valider ou refuser les transactions au sein de la chaîne de blocs. Il est notamment indispensable pour assurer la cohérence des données et l'intégrité de la chaîne contre des modifications frauduleuses.

4. ***Le registre ou la chaîne de blocs*** : la « blockchain » est organisée sous forme d'une chaîne de blocs contrairement aux systèmes de base de données traditionnels, qui contiennent les transactions effectuées au sein du système. Cette structure permet de garantir l'immuabilité des données.
5. ***Les règles de validation*** : La « blockchain » dispose d'un fonctionnement interne qui est propre à son implémentation. Afin de rester agnostiques à toute implémentation spécifique, nous n'avons pas pleinement couvert cet aspect au sein de cette partie. Nous expliciterons plus en détail ce concept dans la partie « Analyses et développement » de ce rapport, notamment via le concept de « smart contract ».

La compréhension des concepts fondamentaux, inhérents au fonctionnement d'une blockchain, nous permet de faire la synthèse de ces apports et limites en tant que technologie de stockage et de diffusion d'information au sein d'un système informatisé.

3.1.3 Apports et limites de la technologie

Au même titre que de trouver une définition unique pour le terme « blockchain », l'identification des apports et des limites de la technologie est un exercice complexe. La littérature propose un grand nombre de travaux s'efforçant de qualifier les apports de la technologie. Il est cependant important de noter que les caractéristiques identifiées sont fortement dépendantes du type de « blockchain » que l'on souhaite analyser.

A Avantages et apports

« Garrick Hileman et Michel Rauchs » considèrent que la « blockchain » est une technologie pertinente lorsque l'on souhaite atteindre l'un des objectifs suivant (Hileman & Rauchs, 2017) :

Tableau 4: Apports de la blockchain au sein d'un système (Hileman & Rauchs, 2017)

Avantage	Description
Réduire le besoin de confiance entre les parties prenantes	Réduire le besoin de « confiance » entre les parties prenantes d'un système en déposant la « confiance » sur le système. Par sa nature, la « blockchain » permet de mettre en place un système autonome, qui réduit drastiquement la nécessité d'une intervention tierce ou humaine. Cela se traduit par un système plus transparent et égalitaire, qui permet aux différents acteurs d'interagir avec ce dernier en réduisant les possibilités de fraude (doit être nuancé dans le cadre d'une blockchain « privée »).
Construire un système de transfert de valeur sûre	Le caractère immuable des transactions au sein de la « blockchain » offre une garantit concernant l'intégrité et la pérennité des données stockées. Elles permettent notamment au système de délivrer un « registre » fiable de toutes les opérations ayant été effectuées au sein du système.
Rationalisez les processus métier sur plusieurs entités	L'architecture « décentralisée » et « distribuée » des systèmes « blockchain » permet de déporter les processus métier sur l'ensemble des nœuds du réseau, tout en garantissant leurs authenticités .
Augmenter la transparence et l'auditabilité	La structure et l'organisation de la chaîne de blocs permettent à quiconque de vérifier son authenticité. Par nature, cette structure permet de prouver le moment, l'ordre et l'objet d'une transaction sans aucune ambiguïté. Les données stockées au sein de la « blockchain » peuvent être facilement consultables par les participants du réseau (doit être nuancé dans le cadre d'une blockchain « privée »).

Nous retrouvons la totalité de ces mêmes bénéfices au sein d'un article faisant état des avantages de la « blockchain » dans le domaine des assurances et de la finance. (Gatteschi et al., 2018). Ces aspects étant directement liés au fonctionnement de la technologie, une étude analysant l'impact de la « blockchain » en tant que plateforme d'achats et revente d'énergie identifie précisément les mêmes avantages à l'utilisation de cette technologie. En effet, après l'implémentation du système et l'analyse des résultats obtenus, l'étude démontre que la « blockchain » apporte : *un environnement distribué et sûr ; de la transparence et de la fiabilité ; une absence d'autorité centrale pour contrôler le système ; une immuabilité des transactions et un coût par transaction plus faible que dans les systèmes traditionnels*. Finalement, dans un ouvrage intitulé « La blockchain, ou la confiance distribuée », les auteurs « Yves Caseau et Serge Soudoplatoff » (2016) identifient les cinq promesses faîtes par la « blockchain » comme étant : la confiance distribuée ; un système transactionnel fiable; la validation des données par une large communauté ; l'absence de tiers de confiance ; l'exécution autonome de protocole complexe. Selon leurs analyses, la pertinence de la blockchain réside dans la combinaison et dans la présence de ces cinq facteurs simultanément. Ils considèrent que l'absence de ces cinq conditions-cadres ne justifierait pas la mise en place d'un écosystème basé sur la blockchain, car le coût non négligeable de sa mise en place peut être remplacé par des systèmes plus simples et efficaces (Soudoplatoff & Caseau, 2016).

Nous constatons donc que les travaux faisant état des avantages de la « blockchain » semblent tous être en accord sur les principaux atouts de cette technologie. Nous pouvons donc affirmer que bien que la technologie soit encore à un stade d'adoption au sein des différents secteurs d'activité, les enjeux et atouts liés à sa nature semblent être clairement identifiés. Afin de produire une synthèse des apports et des limites de la technologie, nous allons maintenant nous intéresser aux inconvénients inhérents à l'implémentation de la « blockchain ».

B Inconvénients et limites

Pour conserver la cohérence de l'argumentaire, nous avons privilégié les études sélectionnées pour identifier les apports et avantages de la technologie « blockchain » afin d'en extraire leurs analyses concernant les limitations de cette dernière. L'étude menée par « Garrick Hileman et Michel Rauchs » présente un sondage réalisé à l'aide d'un panel de 200 participants ayant déjà utilisé ou implémenté la technologie « blockchain ». Le sondage identifie les principaux obstacles à l'adoption de la technologie, selon la perspective des participants. Les critères suivants ont été identifiés (le premier étant l'obstacle le plus important et le dernier le moins significatif) :

Tableau 5: Freins à l'adoption de la technologie "blockchain" (Hileman & Rauchs, 2017)

Freins à l'adoption de la technologie	Description
Risques juridiques et cadres réglementaires	L'absence d'un cadre légal « clair » et bien défini (protection des données, valeur juridique des « smart contract ») est une problématique fondamentale qui entrave l'adoption de la technologie.
Confidentialité	La transparence qui caractérise le fonctionnement des « blockchain » publiques est à la fois un avantage et un frein. En effet, certains secteurs doivent garantir un haut degré de confidentialité vis-à-vis de leurs clients (ex. : secteur bancaire, médical). Les blockchain « privées » semblent être plus appropriées pour ces cas d'utilisation.
Réticence à changer les processus opérationnels établis	L'implémentation de la technologie au sein de systèmes existants représente un coût non négligeable. En effet, les changements induits par l'introduction de la « blockchain » peuvent être perçus comme « trop coûteux » par rapport aux

	avantages qu'elle pourrait amener.
Maturité de la technologie	La technologie n'est pas encore perçue comme étant assez stable pour être implémentée en production.
Difficulté à construire un réseau d'affaires	Faisant partie des attentes suscitées par la technologie, il semblerait que la construction d'un réseau entre plusieurs parties prenantes (entreprises ou entités commerciales) ne soit pas une tâche aisée.
Conflits potentiels avec les lois sur la protection des données	Les contraintes imposées par les lois sur la protection des données dans certains pays peuvent être incompatibles avec les concepts fondamentaux de la technologie (immuabilité, impossibilité de supprimer une transaction).
Problèmes de performances et d'évolutivité du système	Les coûts de transactions (en termes de temps et de puissance de calculs), souvent liées au mécanisme de « consensus » implémenté peuvent être un problème sur des systèmes complexes.
Réticence à abandonner un certain niveau de contrôle	L'autonomie qui caractérise le fonctionnement des « blockchain » publiques est à la fois un avantage et un frein. En effet, la perte de contrôle sur le pilotage du système n'est pas toujours la bienvenue. Les blockchain « privées » peuvent résoudre certaines de ces problématiques.
Problèmes de sécurités	L'apparition d'éventuelles failles de sécurités au sein de la blockchain interroge sur les moyens à disposition pour les résoudre.

Les freins identifiés dans le tableau ci-dessus sont révélateurs. En effet, nous pouvons identifier des problématiques qui concernent directement la technologie (ex. : problèmes de sécurité, de performances ou d'évolutivité), mais également des problèmes d'autres natures. Les problèmes liés aux lois sur la protection des données, sur les législations, les cadres légaux ou encore à la confidentialité sont des problématiques qui sont fortement corrélées à l'environnement (géographique, politique ou économique) dans lequel sera déployée la technologie. Nous pouvons d'ores et déjà affirmer qu'une analyse approfondie de l'environnement et de l'écosystème, dans lequel on souhaite implémenter la blockchain, est nécessaire afin de réduire au maximum les risques d'échecs liés à ces facteurs. Le tableau permet également d'extraire un troisième type de problématique qui est directement lié au changement de paradigme imposé par la technologie. Si les promesses et les champs d'applications semblent très prometteurs, certains freins cités ci-dessus trahissent une certaine peur du changement des processus établis. En effet, la réticence à abandonner le « contrôle » du système montre la volonté que peuvent avoir les entités à maîtriser les tenants et les aboutissants de leur environnement. L'idée de déporter cette maîtrise au sein d'un système autonome peut créer un sentiment de frustration ou de perte de maîtrise sur son système. Ces facteurs doivent être pris en compte lors de l'adoption d'une technologie souvent classée comme « disruptive[4] ». L'étude analysant l'impact de la « blockchain » en tant que plateforme d'achats et revente d'énergie semble être en parfait accord avec les freins cités ci-dessus. Si la liste est moins exhaustive, elle relève notamment les désavantages suivants: complexité de la technologie et « challenges » non résolus ; problèmes d'évolutivité sur des systèmes complexes ; immaturité de la technologie ; appréhension ou réticente sociale à l'adoption de la technologie ; consommation d'énergie élevée (Mengelkamp et al., 2018). Concernant l'étude analysant les impacts de la blockchain dans les secteurs financiers et des assurances, le constat est drastiquement le même. Le problème de consommation d'énergie, lié à l'utilisation de certains mécanismes de « consensus », est le premier désavantage cité. Nous retrouvons également les problèmes liés à la protection des données et à la confidentialité. L'étude identifie également des problèmes liés à l'espace disque consommé par les données. En effet, dans le contexte d'une blockchain

4 Technologie qui perturbe ou menace de changer les modèles et pratiques établies au sein d'un système, un marché ou un secteur d'activité (Pezet, 2017).

publique et dans un système « distribué », chaque participant possède sa propre version de la chaîne de blocs en local. De ce fait, elle est directement impactée par la taille des données contenues dans la « blockchain » (à titre d'information, la blockchain « Bitcoin » a atteint une taille d'environ 260GB en 2020 (Blockchain.com, 2020a)). Cette problématique nous semble en effet pertinente à prendre en compte selon le type de système analysé. La dernière problématique soulevée concerne l'implémentation et le fonctionnement des « smart contracts ». En effet, ces portions de codes exécutées à chaque transaction ne sont pas à l'abri de contenir du code malveillant ou non fonctionnel. Cela pourrait engendrer des erreurs graves au sein des transactions et susciter de la méfiance vis-à-vis du système, de la part des participants (Gatteschi et al., 2018).

À l'aide des informations récoltées, nous sommes en mesure de réaliser une synthèse des principaux avantages et inconvénients, liés à la technologie blockchain, ayant été récoltée dans la littérature scientifique et spécialisée.

Tableau 6: Synthèse des apports et des limites de la technologie "blockchain" dans un système

Avantages	Inconvénients
Niveau de « confiance » accrue	Performances et évolutivité non garanties
Contrôle autonome et réduction des intermédiaires	Niveau de maturité insuffisant
Transparence et auditabilité des transactions	Potentiellement en inadéquation avec certaines législations et avec la loi sur la protection des données
Stockage et partage de l'information de manière « distribuée » et « décentralisée »	Consommation élevée de ressources (électricité et puissance de calcul) en fonction du « consensus » implémenté
Fiabilité et immuabilité des données	Induis un changement de paradigme important
Automatisation de processus complexes (« smart contracts »)	

La synthèse que nous présentons, à défaut d'être exhaustive, semble être en adéquation avec les éléments identifiés dans la littérature et tente de rester agnostique à toute implémentation ou type de blockchain spécifique. Elle peut servir de base de réflexion pour analyser les besoins d'un système et statuer sur la pertinence de la technologie blockchain dans ce dernier. Afin de clôturer notre revue de la littérature, nous allons analyser plus spécifiquement la pertinence de la blockchain dans le contexte de la mobilité électrique, et plus largement dans le secteur énergétique afin d'en déterminer les potentiels cas d'utilisation.

3.2 La « Blockchain » dans le contexte de la mobilité électrique

Le secteur énergétique fait partie des innombrables secteurs d'activités régulièrement cités lorsque l'on s'intéresse aux potentielles applications de la technologie « blockchain ». À défaut de ne pas figurer, selon « Gartner », parmi les secteurs suscitant le plus d'engouement dans les années à venir, la littérature scientifique et les revues spécialisées font étant d'un grand nombre d'initiatives menées à ce jour (Rimol, 2019).

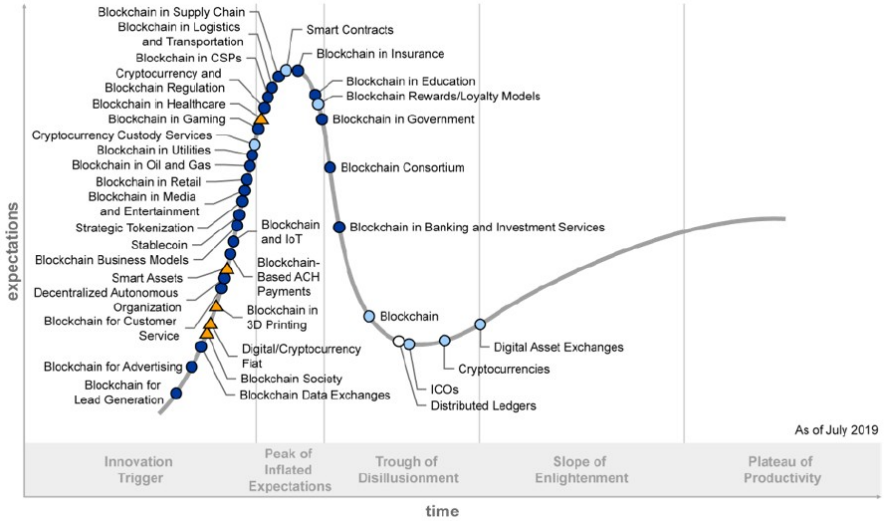


Figure 10: Courbe des secteurs d'activités les plus intéressé par la technologie "blockchain" (Rimol, 2019)

Afin d'illustrer l'intérêt porté par le secteur de l'énergie pour la technologie « Blockchain », nous allons présenter de manière succincte quelques projets ayant un lien direct avec le secteur énergétique suisse. Ces exemples nous permettent également de valider la pertinence de notre thématique en démontrant les efforts réalisés par les acteurs de ce segment afin d'intégrer cette technologie.

3.2.1 Exemples existants

A Energy Web Foundation

L'« Energy Web Foundation » est sans aucun doute le projet le plus ambitieux, dans le cadre de l'implémentation de la « blockchain » au sein du secteur énergétique, que nous ayons identifié dans la littérature sur le plan nationale. Cette fondation à but non lucratif a pour objectif principal d'accélérer l'adoption de la technologie « blockchain » au sein du secteur énergétique suisse et mondiale. Elle compte parmi ces membres des entreprises d'envergure nationale et internationale telles que : « Swisspower » ; « Energy Wasser Bern » ; « Total » ; « ENGIE » et bien d'autres (Energy Web Foundation, 2020). Pour ce faire, elle a mis en place un réseau « public » basé sur la technologie « blockchain » destiné à supporter une multitude d'applications en lien avec le domaine de l'énergie. L'infrastructure se repose sur la plateforme « Ethereum » tout en améliorant les performances et l'évolutivité du réseau en implémentant un mécanisme de « consensus » basé sur la « Proof-of-Authority ». La fondation, basée à Zoug, bénéficie d'un soutien de poids de la part de services industriels basé à Genève, Lausanne ou Berne (Queijo, 2017).

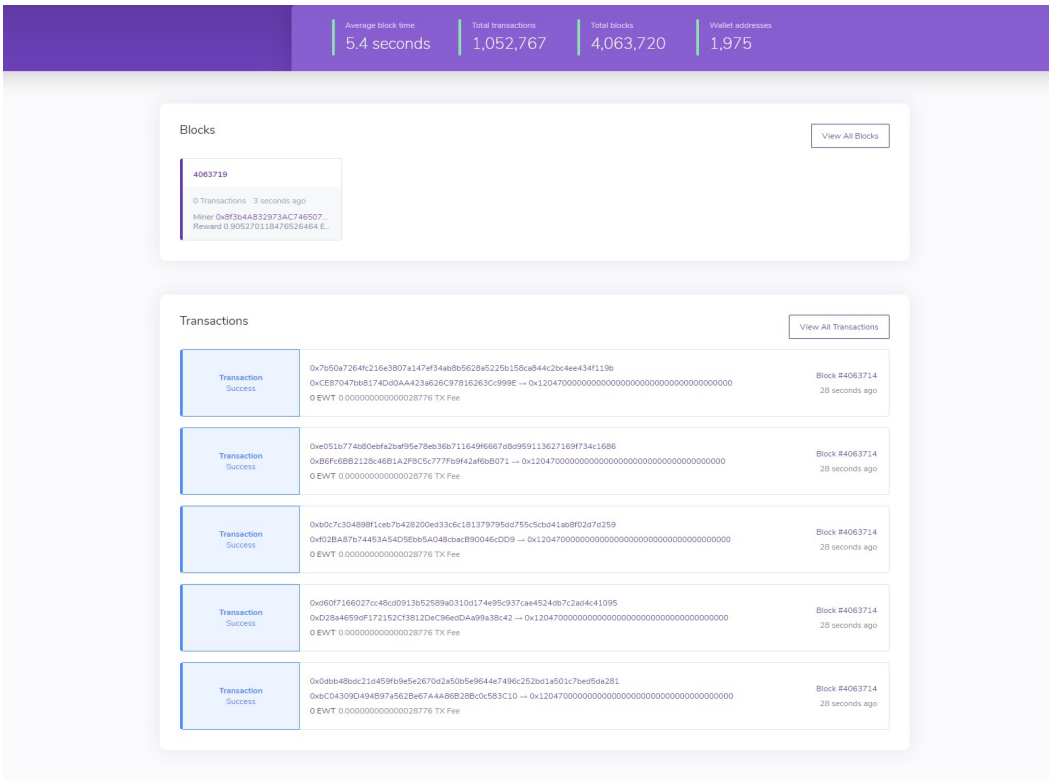


Figure 11: Visualisation du réseau "blockchain" de la "Energy Web Foundation"

Cette « blockchain » comptabilise à ce jour 13 applications dédiées qui reposent sur son fonctionnement et tous en lien avec le secteur énergétique.

B SwissPower – EWB

Le service industriel « Energie Wasser Bern » fait partie des acteurs nationaux très actifs dans la promotion et le test de la technologie « blockchain ». Elle a notamment testé, dans le courant de l'année 2019, un nouveau système destiné à recharger les véhicules électriques au travers de la « blockchain ». Cette infrastructure se base sur la « blockchain » présentée ci-dessus, à savoir l'« Energy Web Chain ». Ce projet pilote vise à homogénéiser l'expérience inhérente au processus de rechargement des véhicules électriques en proposant une plateforme centralisée basée sur la technologie « blockchain ». Cette simplification de l'expérience vise à améliorer la diffusion de la mobilité électrique et à réduire les coûts inhérents aux frais de transaction qui sont trop élevés au sein des systèmes traditionnels. Le projet est aujourd'hui encore en phase de tests auprès des employés de la société bernoise. Elle utilise notamment l'application « Share&Charge », elle aussi basée sur la blockchain de la « Energy Web Foundation » (Wagner, 2019).

La « EWB » est également impliquée dans un autre projet lié à l'implémentation de la « blockchain » au sein du secteur énergétique, en collaboration avec « PosteFinance ». Baptisé « Blockchain for Utility (B4U) », ce projet vise à promouvoir les sociétés d'autoconsommation basée sur la « blockchain ». Cette infrastructure est quant à elle basée sur la plateforme « Hyperldeger Fabric » (Foucault-Dumas, 2018).

Nous pouvons compléter notre liste d'exemples avec des systèmes tels que « Prosume » et « Hive Power » qui visent à implémenter une plateforme d'échange de « kWh » au sein d'un réseau d'autoconsommation et d'autoproduction ou encore « Poseidon » qui cible le calcul de l'empreinte carbone produite par les objets.

4 Analyses et développement

Nous allons aborder la phase d'analyse et de développement de cette étude en nous basant sur les informations et connaissances récoltées lors de notre revue de la littérature. En effet, nous avons été en mesure de définir les concepts tournant autour de la technologie « blockchain » et de présenter des exemples concrets d'implémentation au sein de secteurs d'activités liés au domaine énergétique. Ce chapitre va dans un premier temps présenter l'implémentation qui sera mise en place dans le cadre de ce travail et qui servira également de « POC » afin de démontrer la pertinence de la technologie. Nous procéderons, suite à cette présentation, à l'élaboration des critères de sélection de la plateforme « blockchain » et à la sélection de cette dernière à proprement dit. Nous clôturerons notre analyse par la présentation du système implémenté et des résultats obtenus.

4.1 Architecture et objectifs du projet

Pour être en mesure d'illustrer le potentiel de la technologie dans le cadre de la mobilité électrique, nous devons mettre en place un système qui soit capable de supporter les processus de consommation énergétique actuels. L'entreprise d'audit et de conseil « PwC » a réalisé une étude démontrant l'organisation du marché de l'énergie traditionnel, avant l'avènement de la « blockchain ».

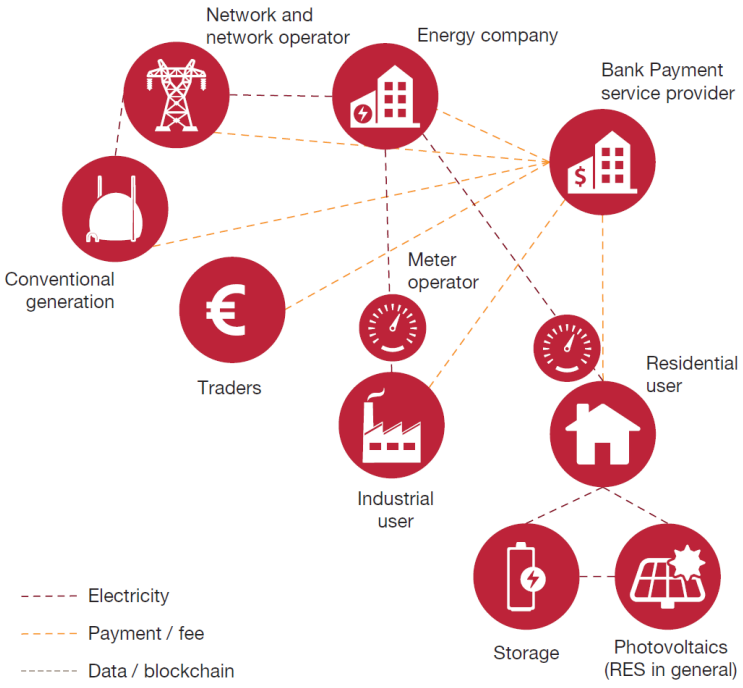


Figure 12: Structure traditionnelle du marché de l'énérgie

Sans nous attarder sur l'ensemble du modèle, nous pouvons constater que la consommation d'énergie est traditionnellement régulée par un modèle « fournisseur/consommateur ». Dans ce modèle, le consommateur (entreprise ou particulier) consomme un certain nombre de « kWh » sur le réseau. L'énergie consommée peut venir du réseau principal (gérée par une entreprise ou fournisseur un d'énergie) ou provenir de sources personnelles (ex. : batteries, panneaux solaires) si le consommateur en possède. Dans le premier cas de figure,

le consommateur utilise un certain nombre de « kWh » qui seront comptabilisés par un « compteur » et qui serviront de bases pour la facturation du service, établie par le fournisseur. Dans le deuxième cas de figure, le consommateur se trouvera dans une situation d'autoconsommation. Ce modèle nous permet d'identifier trois rôles majeurs au sein du processus de consommation : *le consommateur ; le fournisseur et le compteur*.

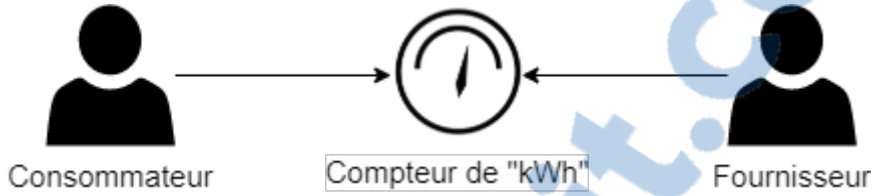


Figure 13: Acteurs du modèle de consommation d'énergie traditionnel

Nous devons donc tenir compte de ces trois rôles au sein de notre système afin de proposer une implémentation qui soit proche de la réalité du terrain. Pour ce faire, nous souhaitons mettre en place le processus suivant :

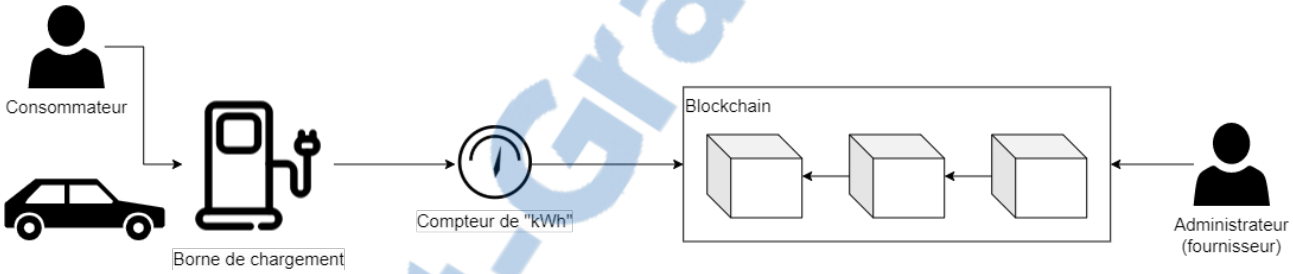


Figure 14: Fonctionnement de notre système "Proof-of-Concept"

Nous devons mettre en place un système basé sur la « blockchain » capable de stocker les informations relatives à une transaction (un rechargement) réalisée par le consommateur. Dans ce système, le consommateur procédera au rechargement du véhicule via une borne de chargement. Une fois le processus de chargement terminé, le compteur récoltera les informations concernant le rechargement (ex. : « kWh » consommés, source utilisée) et les transmettra à notre système « blockchain » qui stockera l'information de manière immuable. Du point de vue de l'administrateur (ou fournisseur), il sera en mesure de gérer (ajouter, modifier ou supprimer) les bornes de rechargement au sein du système. Il pourra également consulter les transactions relatives à une borne ou à un consommateur en particulier. Ces manipulations devront être réalisées depuis une interface utilisateur dédiée (nous avons choisi une interface « web » afin de simplifier le développement) pour maximiser l'accessibilité de l'application. Afin d'illustrer le processus dans son ensemble, nous avons mis en place le diagramme de séquence suivant :

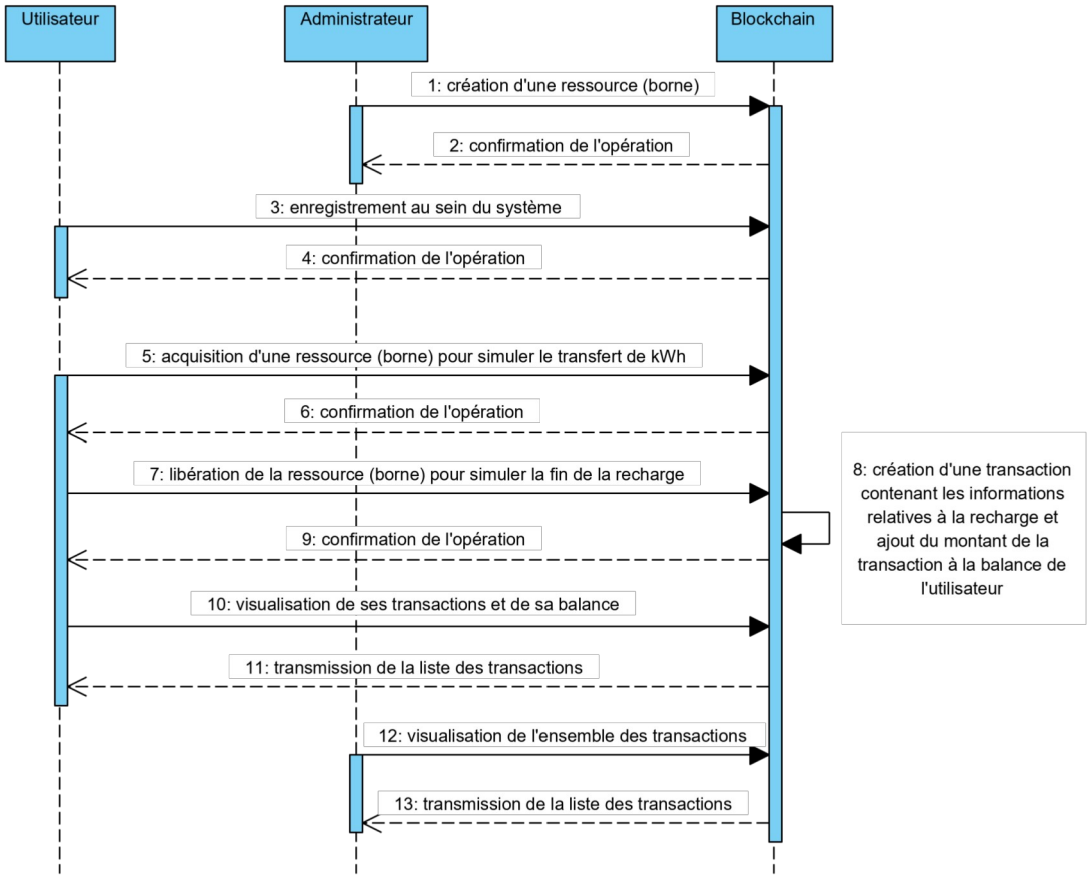


Figure 15: Diagramme de séquence représentant notre cas d'utilisation

Il illustre les opérations que nous souhaiterions pouvoir réaliser au sein de notre système, afin de prouver son fonctionnement dans le contexte de la mobilité électrique. Néanmoins, nous devons d'ores et déjà établir un certain nombre de concepts qui ne seront pas abordés dans le cadre de notre projet. Les notions relatives aux paiements des transactions ne seront pas abordées lors de ce travail. Nous considérons que l'implémentation d'un tel système serait trop coûteuse en temps par rapport à son apport dans le contexte de notre étude. De plus, ne disposant pas de borne de chargement lors de notre implémentation, nous simulerons cette notion directement au sein du système « blockchain » afin de pouvoir visualiser les informations pertinentes. Le processus de communication entre la borne de chargement et un système « blockchain » est crucial pour le fonctionnement de notre système. Étant conscient que nous ne serons pas en mesure de le démontrer dans les temps impartis, nous nous reposons sur les résultats obtenus par Vianin (2018) lors de sa thèse qui démontrent que la communication entre une borne est une plateforme « blockchain » est possible (Vianin, 2018).

Nous allons à présent analyser les différentes solutions existantes sur le marché afin de sélectionner la technologie « blockchain » la plus adaptée à notre cas d'utilisation.

4.2 Choix de la technologie « Blockchain »

Il existe aujourd'hui une multitude d'implémentations de la « blockchain ». Le succès rencontré par cette technologie lors des dernières années a considérablement fait croître et diversifié le marché. Une revue

complète de l'ensemble des solutions existantes nous semble être un exercice compliqué, fastidieux et peu pertinent dans le cadre de cette étude. Nous avons donc présélectionné un ensemble de dix implémentations de la « blockchain », figurant parmi les solutions les plus citées dans la littérature scientifique et spécialisée. Pour réaliser ce travail, nous avons dans un premier temps effectué des recherches sur internet et dans les bases de données académiques afin de trouver des articles, revues, rapports ou thèses dressant un panorama des technologies « blockchain » existantes. Une fois les articles analysés, nous avons retenu trois documents afin d'en ressortir les technologies citées et les comparer au sein de notre travail. Nous avons notamment veillé à ce que les articles retenus aient moins d'un an (basé sur la date de publication) afin d'obtenir un panel d'implémentation basé sur des technologies actuelles.

Tableau 7: Études utilisées pour la sélection des plateformes "blockchain"

Titre	Description
Comparison of blockchain platforms: a systematic review and healthcare examples (Kuo et al., 2019)	Étude comparative entre dix plateformes « blockchain » sélectionnées sur la base d'un score de « popularité » élaboré au sein de l'étude. Les plateformes retenues sont ensuite mises en corrélation avec le secteur de la santé.
Blockchain technology in the energy sector: A systematic review of challenges and opportunities (Andoni et al., 2019)	Étude réalisant une revue systématique évaluant le potentiel de la technologie « blockchain » au sein du secteur énergétique.
Top 10 blockchain platforms you need to know about (Sharma, 2019a)	Article faisant l'élicitation de dix plateformes « blockchain » jugées dignes d'attention au cours de l'année 2019

Nous avons sélectionné dix plateformes, toutes ayant été citées au moins une fois au sein des documents présentés ci-dessus. Pour rendre la sélection pertinente dans le cadre de notre étude, nous avons appliqué deux critères de manière successive (par ordre d'importance).

Tableau 8: Critères de sélection utilisés pour le choix des plateformes "blockchain"

Critère	Points attribués
Plateformes citées dans le contexte du secteur énergétique	3
Plateformes citées dans « x » nombres d'études (maximum 3 points)	1-3

Ce processus de sélection nous permet de mettre en avant les plateformes ayant été citées ou implémentées dans le contexte du secteur énergétique tout en prenant en compte leur « popularité » (nombre d'occurrences) au sein des différentes études. L'application de ce processus nous permet de mettre en évidence les dix plateformes « blockchain » suivantes (les plateformes restantes ayant été citées et non retenues ont obtenu le score de 1) :

Tableau 9: Plateformes "blockchain" retenues pour notre étude

Plateforme	Score
Ethereum	6
Hyperledger	6

MultiChain	6
LiteCoin	5
Interbit	4
Energy Web	4
Tendermint - Cosmos	4
Keyless signature Infrastructure (KSI)	4
Qtum	4
Ripple	2

Les plateformes précédemment citées seront comparées selon les critères de sélections que nous identifierons lors du prochain chapitre. Les résultats obtenus suite à cette comparaison nous permettront de sélectionner la ou les plateformes les plus pertinentes dans le cadre de notre implémentation.

4.2.1 Mise en place des critères de sélection pertinents

Lors de notre revue de la littérature, nous avons identifié les principaux composants constituant la technologie « blockchain ». Nous avons pu mettre en lumière certains concepts tels que : la distribution ; les consensus ou les « smart contract ». Ces composants sont indéniablement essentiels à la compréhension du système et nous aident à identifier les critères fondamentaux à la sélection d'une implémentation de la « blockchain » sûre et efficiente. Néanmoins, ils ne sont pas suffisants pour garantir que l'ensemble des besoins de notre système soient couverts. L'étude menée par Kuo et al. (2019) définit un certain nombre de critères à prendre en compte lors de la sélection d'une plateforme « blockchain ». Elle cite notamment les éléments suivants : *les permissions au sein du réseau ; le mécanisme de « consensus » ; l'équipement matériel nécessaire ; le support des « smart contracts » ; les conditions d'utilisations de la plateforme (licence) et les langages de programmation supportés*. De la même manière, Hileman et Rauchs (2017) tentent de mettre en avant les principaux « blocs » faisant partie d'un écosystème basé sur la « blockchain ». Ils définissent quatre axes qui doivent être analysés pour être en mesure de sélectionner une plateforme qui soit en adéquation avec les besoins d'un système.

Tableau 10: Principaux "blocs" faisant partie d'un système "blockchain" (Hileman & Rauchs, 2017)

Axe	Interrogations
Diffusion des données	• Comment les données sont-elles propagées au sein du réseau ?
	• Qui reçoit et qui peut consulter les données ?
Stockage des données	• Quel type de données sont stockées dans la chaîne ?
	• Y a-t-il des données stockées en dehors de la chaîne ?
Mécanisme de « consensus »	• Comment le « consensus » est-il obtenu ?
	• Sur quels critères se base le « consensus »
	• Qui est impliqué dans le processus ?
Support des « smart contracts »	• La plateforme supporte-t-elle les « smart contracts »

- Qu'elles sont les couches qui supportent cette fonctionnalité

Nous pouvons d'ores et déjà identifier que les deux études semblent mettre en lumière un grand nombre de critères de sélection communs. Afin de pouvoir comparer les plateformes retenues au sein de notre étude, nous allons synthétiser les critères que nous venons d'identifier et définir les points de comparaisons suivants :

Tableau 11: Critères sélectionnés pour le comparatif des solutions retenues

Critère	Description
Architecture et permissions	Comparer les différents types d'architectures existants et les niveaux des permissions possibles au sein d'un réseau basé sur la « blockchain ».
Nature et stockage des données	Identifier et analyser les différents modèles de stockage de données existants au sein d'un écosystème « blockchain », tout en tenant compte du type de données contenues dans notre système.
Mécanismes de « consensus »	Identifier et analyser les types de « consensus » existant et sélectionner un mécanise qui soient en adéquation avec les besoins de notre système.
« Smart contracts »	Définir la notion de « smart contracts » et analyser la pertinence et la nécessitée de cette fonctionnalité au sein de notre implémentation.
Licence	Type de licence associé à l'utilisation de la plateforme
Prix	Investissement financier nécessaire à l'acquisition et à l'exploitation de la plateforme
Popularité	Nombre de contributeurs (si disponible)

Maintenant que nous avons identifié les critères de sélections pertinents au choix d'une implémentation « blockchain », nous allons les analyser plus en profondeur afin d'en comprendre les tenants et aboutissants.

A Architecture et permissions

La technologie « blockchain » a considérablement évolué depuis l'avènement de sa première implémentation public, le « Bitcoin ». Dans un premier temps, le succès du « Bitcoin » à contribué à la naissance de plusieurs implémentations de la « blockchain » étant toute basée sur le même modèle : la création d'un nouvel écosystème financier public par la définition d'une nouvelle cryptomonnaie (devise). Cependant, la recherche s'est rapidement intéressée au fonctionnement de la « blockchain » et a contribué à identifier le potentiel de cette technologie hors des champs d'applications strictement financiers. Aujourd'hui, il existe un certain nombre d'implémentations de la « blockchain » permettant d'adapter son fonctionnement afin de le rendre compatible avec des domaines d'activités divers et variés. Nous avons identifié les principaux modèles architecturaux ou paradigmes récurrents dans la littérature scientifique et spécialisée.

Tableau 12: Modèles d'implémentations possibles de la "blockchain" (Viriyasitavat & Hoonsopon, 2019)

Modèle	Description
Public	Le modèle « Public » est le modèle originellement adopté par les premières implémentations de la « blockchain » (ex. : Bitcoin, Ethereum). Il a la particularité d'être totalement ouvert et autonome une fois déployée. En effet, quiconque souhaite rejoindre un réseau « Public » peut le faire sans aucune restriction et accéder à l'ensemble des informations contenues au sein de la

	chaîne. La notion de « tiers de confiance » est ici totalement absente. Chaque membre du réseau dispose des mêmes droits. Ce modèle est particulièrement utilisé dans le contexte des cryptomonnaies et est pertinent lorsque les membres du réseau ne sont pas connus et doivent avoir accès à l'ensemble des informations.
Privé	Le modèle « Privé », au contraire du modèle « Public » introduit une notion de validation et d'autorisation des nœuds ayant droit à faire partie du système. Dans le contexte d'une blockchain « Privé », un administrateur est nécessaire afin de configurer les accès pour chaque membre du réseau. Une personne ne disposant pas des droits d'accès nécessaire ne pourra pas participer au réseau. La notion de « tiers de confiance » est ici indispensable. Ce modèle est pertinent lorsque le réseau et les participants de ce dernier sont connus à l'avance et que le niveau d'accès aux données doit être contrôlé.
Autorisé (à permissions)	La littérature cite souvent le modèle « Autorisé » ou « À permissions » sur le même plan que les deux autres. Il est perçu comme étant une composition hybride entre les deux modèles précédents. Il vise à établir un réseau public permettant à quiconque de rejoindre le réseau librement. Cependant, le réseau embarque également, à l'instar du modèle « Privé », un mécanisme de permissions limitant l'accès à certaines informations ou fonctionnalités aux participants n'ayant pas les droits nécessaires. Ce modèle est pertinent lorsque l'ensemble des participants n'est pas connu à l'avance, mais que les administrateurs du réseau, eux, le sont.

Ces modèles d'implémentations permettent de couvrir un large nombre d'applications possibles au sein de divers secteurs d'activité existants, y compris le secteur énergétique et plus particulièrement celui de la mobilité électrique. La définition des modèles existants aujourd'hui nous permet d'identifier un certain nombre de critères indispensables à prendre en compte lors de la sélection d'une technologie particulière. En effet, nous avons pu identifier deux notions primordiales qui doivent être identifiées au sein de notre implémentation : *l'accès au réseau et les permissions des participants*. Dans leur étude comparative des différents éléments composant un système « blockchain », « Hileman et Rauchs » tente de classifier les types de « blockchains » existant en fonction de leurs architectures et de l'implémentation d'un système de permissions ou non.

Tableau 13: Types de "blockchain" basé sur leurs modèles de permission (Hileman & Rauchs, 2017)

Type	Accès en lecture	Accès en écriture	Validation des transactions	Exemple
Public (sans permissions)	Tous les participants	Tous les participants	Tous les participants	Bitcoin, Ethereum
Public (avec permissions)	Tous les participants	Participants autorisés	Participants autorisés	EOS, Ripple, Sovrin
Privé (sans permissions)	Participants autorisés	Participants autorisés	Participants autorisés	Holochain, LTO Network, Monet
Privé (avec permissions)	Participants autorisés	Administrateurs du réseau	Administrateurs du réseau	Entreprise Ethereum Alliance, Hyperledger Fabric

Nous avons adapté certaines informations du tableau (daté de 2017) afin que les exemples cités soient plus en adéquation avec les implémentations actuelles (Daniels, 2018). Il reste néanmoins très représentatif des principaux modèles existants au sein des implémentations modernes de la « blockchain ».

Dans le cadre de notre implémentation, nous devons donc nous interroger sur les besoins du système en matière de confidentialité et d'accès à la plateforme pour nous orienter vers une solution qui soit adaptée à nos processus métiers. Nous avons identifié deux types d'utilisateurs au sein de notre système : *les consommateurs et les administrateurs* ; Les consommateurs sont chargés d'interagir avec le système afin de sélectionner une borne et procéder au rechargement de leurs véhicules. Les administrateurs sont chargés d'ajouter ou supprimer des bornes de rechargement au sein du système. Ils doivent également s'occuper des aspects administratifs liés à la facturation des consommateurs.

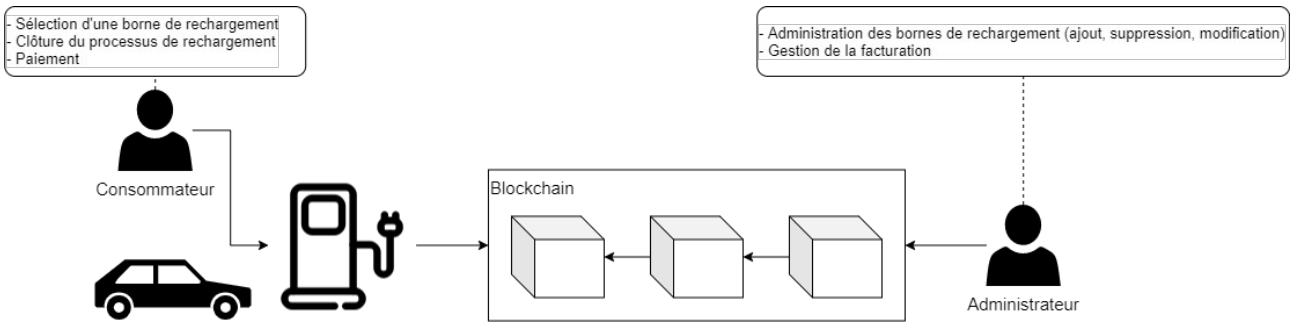


Figure 16: Niveaux de permissions et d'accès de notre système

Nous pouvons donc d'ores et déjà statuer que la notion de « permissions » est nécessaire dans le contexte de notre implémentation. En effet, le consommateur final n'aura pas accès aux mêmes informations et fonctionnalités que l'administrateur du système. Leurs rôles étant diamétralement opposés, nous devons nous orienter vers une technologie qui intègre cette dimension. Concernant les accès à notre plateforme, nous pouvons considérer deux points de vue distincts. Il peut être pertinent de considérer qu'une implémentation « publique » et avec « permissions » soit à terme plus profitable et évolutive dans la mesure où les utilisateurs sont libres de rejoindre le réseau et utiliser les bornes de rechargement sans aucune régulation particulière. Ce modèle permettrait de cibler un plus vaste panel de consommateurs tout en gardant la main mise sur l'administration du système. Dans un autre registre, il peut être pertinent de considérer qu'une implémentation « privée » et avec « permissions » apporte un avantage concurrentiel dans certains modèles d'affaires. Nous pouvons prendre pour exemple l'application de notre système au sein d'un complexe hôtelier ou d'une chaîne de restaurants. Le fait de privatiser l'accès à notre système aux seuls clients de l'établissement peut être un argument de vente et d'attractivité supplémentaire. En effet, dans des domaines du secteur tertiaire proposant de services à durées déterminées, l'exclusivité de ce genre de système pourrait s'avérer être un facteur d'aide à la décision (ou à l'achat) supplémentaire pour les clients (ex. : lors d'un voyage, un client disposant d'un véhicule électrique, pourrait choisir un hôtel doté de notre système au lieu d'un autre afin de recharger de son véhicule durant la nuit). Sur la base de ces deux visions, nous privilégierons les technologies étant basé sur *des modèles « à permissions » et ayant un droit d'accès « public » ou « privé »* lors de notre sélection.

B Nature et stockage des données

La problématique liée à la nature et au processus de stockage des données, au sein d'un système « blockchain », est primordiale pour garantir le bon fonctionnement d'un écosystème. De nos jours, la « donnée » ou « information » tant à devenir un élément central des systèmes actuels et gagne constamment en valeur. Nous avons pu voir émerger ces dernières années des secteurs d'activités totalement dédiées à ce concept, tel que la « Data Science » ou encore le « Machine Learning ». Cela illustre l'importance que nous devons accorder aux données au sein des systèmes actuels et le succès de la « blockchain » ces dernières années n'est pas étranger à cette thématique. En effet, la « blockchain » offre par nature un environnement sûr, intègre et transparent pour les données qui transitent en son sein. Néanmoins, les implémentations de la

« blockchain » modernes proposent une variété de possibilités concernant le stockage des données. Ces options doivent être prises en compte afin de sélectionner la technologie qui soit en mesure d'assimiler la nature des données de notre système. La littérature identifie trois types de stockages possibles dans les implémentations actuelles de la « blockchain ».

Tableau 14: Méthodes de stockage des données au sein de la "blockchain" (Hileman & Rauchs, 2017)

Modèle de stockage	Description
Intégralement dans la chaîne	L'ensemble des données relatives à une transaction sont stockées dans la transaction elle-même, et donc la « blockchain ». L'entièreté de la donnée est donc accessible lors de la consultation des transactions.
Partiellement dans la chaîne	Le processus de stockage est scindé en deux. Une partie des données est directement stockée au sein de la transaction alors que la deuxième partie est stockée au sein d'une source de données externe. La transaction référence néanmoins l'adresse de stockage de la partie « hors chaîne ». Nous pouvons par exemple citer le stockage de documents lourds (ex. : vidéos, fichiers « pdf ») comme étant pertinents pour le stockage « hors chaîne ».
Hors de la chaîne	Les informations relatives à la transaction sont totalement stockées au sein d'une source de données externe. La transaction ne contient que des « empreintes numériques » (« hash ») uniques, référençant la donnée ou le fichier stocké dans la source de données externe. La « blockchain » agit comme simple plateforme de « trading », agnostique à toute forme de logique « métier ».

Les différents modèles de stockage présentés au sein du Tableau 14 nous permettent d'entrevoir les possibilités offertes par les technologies « blockchain » actuelles, notamment en matière de décentralisation de l'information et de confidentialité des données. Ces modèles ont effet émergé afin de palier au principe de « transparence », initialement propulser par les architectures « publiques » et « sans permission », qui n'est pas adapté à tous les secteurs (ex. : secteur bancaire, médical). Les modèles adoptant un mode de stockage « partiel » ou « intégralement » hors de la chaîne se basent sur des techniques de cryptographie (que nous avons abordé lors du chapitre « *Erreur : source de la référence non trouvée - Erreur : source de la référence non trouvée* » qui vont référencer des adresses ou des empreintes numériques (« hash ») uniques (Eberhardt & Tai, 2017).

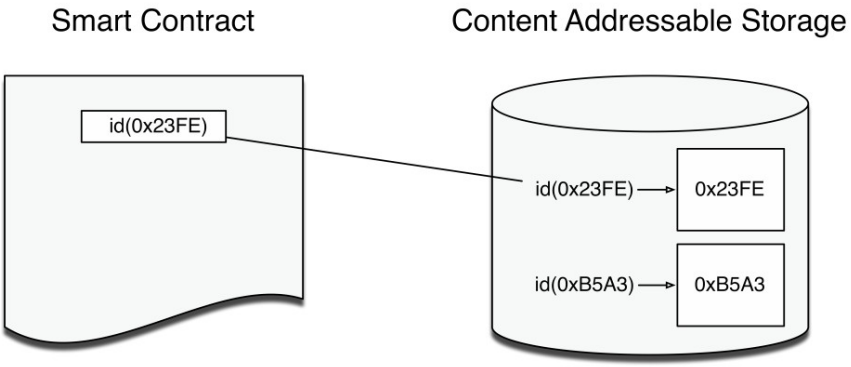


Figure 17: Données stockées dans la "blockchain" dans un modèle "hors chaîne" (Eberhardt & Tai, 2017)

Dans ce genre de modèles, les données sont traditionnellement stockées au sein de systèmes de stockage spécialement conçus pour permettre le référencement de leurs données depuis des systèmes externes (tels que la « blockchain »). Nous pouvons citer des exemples tels que : « IPFS (Protocol Labs, 2020) » ; « Swarm (Swarm, 2020) » ; « Sia (Nebulous, Inc., 2020) » et bien d'autres (Eberhardt & Tai, 2017).

Afin de garantir le bon fonctionnement de notre système, nous devons analyser la nature des données de notre écosystème pour être en mesure de sélectionner le modèle le plus adapté à nos besoins. Une première donnée importante concerne la nature et la structure des informations qui vont transiter au sein du système. Nous avons prévu de mettre en place le modèle de données suivant :

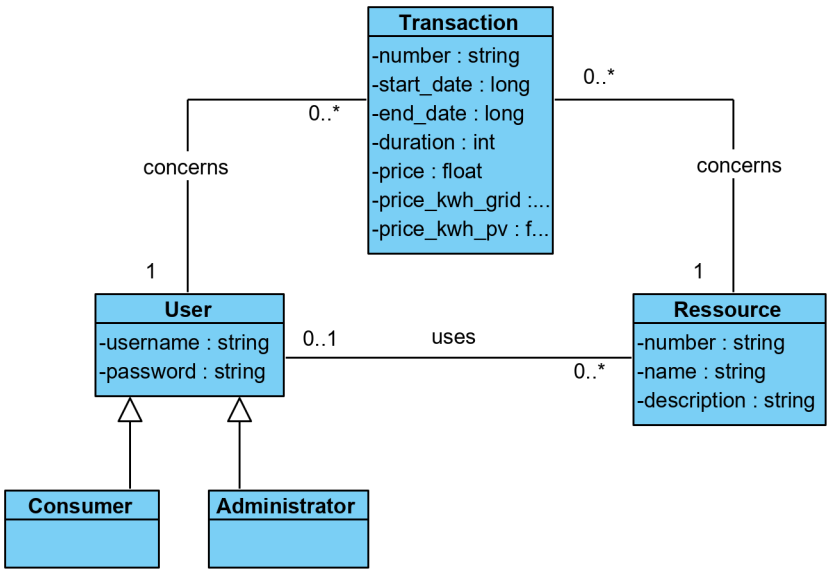


Figure 18: Modèle de données à implémenter au sein de notre système

Nous pouvons constater que les informations qui figurent dans notre modèle sont toutes représentées par des types de données « primaires ». Les données contenues au sein de notre système seront donc essentiellement des données textuelles (type « *string* ») ou numériques (type « *int* », « *long* » et « *float* »). Par conséquent, nous ne nécessitons pas de stocker des fichiers volumineux ou d'autres types de données justifiant l'utilisation d'un support de stockage externe. En parallèle, nous avons également opté pour une solution implémentant une architecture « blockchain » de type « public » ou « privé », qui dispose d'un système de « permissions ». La mise en place d'un système de permissions nous garantit déjà la confidentialité des données au sein de notre système.

En conclusion, dans le cadre de notre implémentation, nous allons opter pour un modèle de stockage « *intégralement dans la chaîne* ».

C Mécanismes de « consensus »

Le mécanisme de « consensus » au sein de la « blockchain » représente sans aucun doute l'un des critères fondamentaux à analyser afin d'obtenir un système sûr et évolutif. Il existe aujourd'hui une multitude de « consensus » disponibles, tous ayant leurs propres avantages et limitations selon l'environnement dans lequel ils évoluent. Il n'est par conséquent pas aisé de répertorier l'ensemble des mécanismes existants. La diversité existante au sein des mécanismes de « consensus » n'est pas anodine. À l'heure actuelle, il n'existe pas de mécanismes « universels » qui soient adaptés à tous les types de systèmes. La littérature spécialisée cite souvent cette problématique comme étant le « trilemme » des blockchains (NeonVest, 2019).

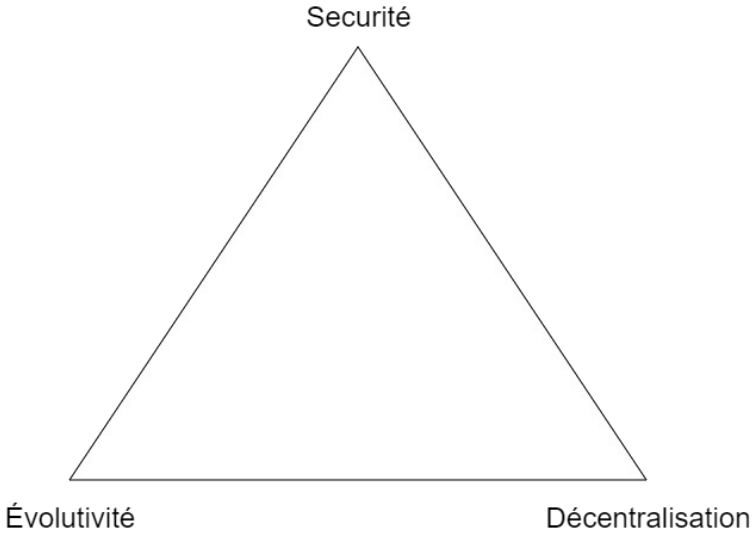


Figure 19: Les trois problématiques majeurs de la "blockchain" (NeonVest, 2019)

La figure présentée ci-dessus illustre les trois axes ou objectifs majeurs que la « blockchain » souhaite solutionner. Néanmoins, dans les implémentations actuelles, il est impossible de pleinement couvrir l'ensemble de ces objectifs simultanément. Cette incapacité à couvrir l'ensemble des objectifs est notamment due à l'absence d'un mécanisme de « consensus » qui soit suffisamment sûr (capable de résister aux attaques), évolutif (performant et applicables à de larges réseaux) et décentralisé (prenant en compte l'ensemble des « noeuds » du réseau). Il est donc nécessaire d'analyser les besoins primaires de notre système pour sélectionner le mécanisme le plus approprié, malgré les inconvénients qui le caractérisent. Pour réaliser ce travail, nous avons priorisé les trois axes de développement sur une échelle de quatre « niveaux » de priorité : *critique* ; *important* ; *neutre* ; *sans importance*. Nous justifions la valeur accordée à chaque axe de développement selon les critères qui nous semblent être prioritaires dans notre implémentation.

Tableau 15: Priorisation des axes de développement importants pour notre système

Axe	Priorité	Justification
Sécurité	important	Nous avons précédemment sélectionné un système se reposant sur une blockchain de type « privée ». Ce choix induit naturellement que les acteurs du système seront connus et dans un environnement contrôlé. De ce fait, le risque d'attaque est amoindri par rapport un environnement « public ». Il est néanmoins important de garantir l'intégrité du système, et donc d'accorder une importante particulière à ce critère.
Évolutivité	critique	Le système a pour objectif de supporter un écosystème qui sera à la fois utilisé par des consommateurs (acteur qui utilise les bornes de rechargement) et des administrateurs (acteur qui gère les bornes de rechargement). Si le nombre d'administrateurs n'est pas très impactant, le système doit impérativement être réactif et performant afin de répondre aux demandes d'un nombre important de consommateurs. Le succès du système repose sur sa capacité à offrir un environnement rapide et stable au consommateur final, afin qu'il puisse recharger son véhicule en éliminant le maximum de contraintes. Ce critère est selon nous indispensable au succès du système.

Décentralisation	neutre	L'utilisation de la technologie « blockchain », au sein de notre système, sera pratiquement « transparente » pour le consommateur final. En effet, il interagira avec le système via une interface (application mobile ou web) qui lui présentera les informations nécessaires au chargement de son véhicule, sans notion particulière liée à la technologie. Il n'est donc pas primordial, à notre sens, que le système soit absolument reparti sur le plus grand nombre de « nœuds » possible. La validation des transactions peut donc être gérée de manière plus « centralisée », sans impacter le confort de l'utilisateur. Nous pensons donc que ce critère doit être pris en compte après les deux autres.

Sur la base de la priorisation effectuée, nous allons sélectionner les mécanismes de « consensus » étant les plus adaptés aux conditions-cadres de notre système. Pour les identifier, nous allons sélectionner les « consensus » les plus récurrents dans la littérature scientifique. Nous avons sélectionné trois études faisant l'état de l'art des mécanismes de « consensus » utilisé par les « blockchains » actuelles. Sur cette base, nous sélectionnerons le ou les mécanismes les plus pertinents dans le cadre de notre implémentation.

Tableau 16: Études sélectionnées pour le comparatif des différents "consensus"

Titre	Description
« Comparative Analysis of Blockchain Consensus Algorithms (Bach et al., 2018)»	Étude comparative entre différents mécanismes de consensus (sélectionnés sur la base de leur implémentation au sein des cryptomonnaies les plus populaires) et le consensus « Proof-of-Work »
« Deconstructing Blockchains: A Comprehensive Survey on Consensus, Membership and Structure (Natoli et al., 2019) »	Étude comparative faisant l'état de l'art des mécanismes de sélection, des consensus et des structures existantes en tant que composants des blockchains actuelles
« Blockchain technology in the energy sector: A systematic review of challenges and opportunities (Andoni et al., 2019) »	Étude réalisant une revue systématique évaluant le potentiel de la technologie « blockchain » au sein du secteur énergétique

Nous avons sélectionné cinq mécanismes (ou familles) de « consensus ». Trois d'entre eux ont été sélectionnés sur la base de leurs récurrences (popularité) dans les études sélectionnée. Nous avons sélectionné les deux « consensus » restant en fonction du potentiel perçus dans le cadre de notre implémentation. Nous pourrons ainsi comparer leurs caractéristiques, selon les trois axes d'analyse définis précédemment. Il est néanmoins important de préciser que nous n'approfondirons pas le fonctionnement technique et algorithmique des « consensus » sélectionné, n'étant pas fondamentalement crucial dans notre processus de décision.

Proof-of-Work (PoW)

Ce mécanisme est historiquement le plus connu et le plus utilisé au sein des blockchains actuelles. En effet, il a été introduit avec l'avènement du « Bitcoin » et est aujourd'hui largement représenté au sein des cryptomonnaies en tant que processus de validation des blocs. Le principe caché derrière le « PoW » est relativement simple. Chaque participant du système souhaitant participer au processus de validation d'un bloc doit résoudre un problème mathématique. Le problème est formulé de telle sorte à ce que la solution soit complexe à trouver (besoin d'une puissance de calcul conséquente, et donc énergivore) et néanmoins

facilement vérifiable par les autres participants (Natoli et al., 2019). Le premier participant ayant trouvé la solution la transmet au système. Le restant des participants doivent ensuite vérifier et valider la solution afin que le bloc soit ajouté à la chaîne. Le vainqueur est donc considéré comme le créateur du bloc et reçoit une contrepartie financière pour sa preuve de travail (Andoni et al., 2019).

La méthode de fonctionnement du « PoW » présente l'avantage d'être complètement « décentralisée » et donc d'offrir l'opportunité à tous les participants du réseau d'être sélectionné pour le processus de validation du bloc. Cela induit que ce « consensus » est particulièrement pertinent dans le cadre d'une blockchain « publique ». En matière de « sécurité », le mécanisme est néanmoins soumis à quelques limites qui doivent être prises en considération. En effet, le calcul de solution et la vérification de cette dernière reposent sur les membres ayant la plus grande puissance de calcul au sein du réseau. De ce fait, si un participant parvenait à obtenir une puissance de calcul cumulée dépassant 51 % de la puissance de calcul totale du réseau, il aurait théoriquement le pouvoir sur l'ensemble du réseau. Si ce scénario semble pratiquement impossible au sein de vastes réseaux (ex. : Bitcoin, Ethereum), il est néanmoins envisageable si le nombre de participants venait à être plus restreint (Garg, 2020). La sécurité est donc accrue plus la taille du réseau est importante. D'un point de vue « évolutivité », le constat est radicalement opposé à celui de la sécurité. La puissance de calcul, et donc l'énergie nécessaire, à la résolution du problème mathématique lors de la validation d'un bloc est proportionnellement liée à la taille de la chaîne et au nombre de participants. Par conséquent, plus la chaîne est grande et plus le temps nécessaire à la résolution du problème est important (ex. : la validation d'un bloc au sein de la blockchain « Bitcoin » nécessite aujourd'hui environ huit minutes (Blockchain.com, 2020b)).

Proof-of-Stake (PoS)

Il existe à ce jour de nombreuses implémentations de ce mécanisme (ex. : « Proof-of-Lock », « Proof-of-Deposit », « Proof-of-Activity », « Delegated Proof-of-Stake », « Proof-of-Burn », etc.). Afin de simplifier la compréhension de ces concepts, nous allons rester focalisés sur l'implémentation de base qu'est « Proof-of-Stake ». Ce mécanisme a directement été pensé pour combler les faiblesses identifiées au sein du consensus « PoW ». En effet, le caractère extrêmement énergivore et le temps de traitement nécessaire à la validation des transactions au sein d'un système « PoW » ont contribué à la naissance d'alternatives moins coûteuses en temps et en ressources. « PoS » tente de solutionner ces deux problématiques par l'introduction d'un nouveau mode de sélection des participants à la validation d'un bloc : *la preuve d'enjeu*. Le mécanisme remplace le principe de résolution de problèmes complexes (qui nécessitait beaucoup de puissance de calcul et de temps) par un principe de dépôt de « valeur », apporté par le participant souhaitant être sélectionné pour la validation du bloc. Concrètement, plus le participant dépose un montant important de « valeur » (généralement utilisés dans le milieu des cryptomonnaies, nous pouvons traduire « valeur » par « montant » de la devise implémentée au sein de la blockchain), plus son vote aura d'influence lors de la validation d'un bloc. Si le participant se montre être « honnête », il gardera sa mise en sa possession. Dans le cas où un comportement frauduleux est détecté, il perdra instantanément le montant qu'il a misé (Natoli et al., 2019).

Le processus mis en avant par « PoS » est extrêmement intéressant en tant qu'alternative au consensus « PoW ». En effet, il garde les avantages apportés par « PoW », notamment en matière de « décentralisation » en permettant à tous les « noeuds » du système de participer au processus de validation d'un bloc. Il apporte également, contrairement à son prédécesseur, un mécanisme moins énergivore et considérablement plus rapide. Cet état de fait contribue à faire de « PoS » un mécanisme nettement plus « évolutif » que « PoW ». Cependant, le système de « mise » ou de dépôt de « valeur » proposé dans ce mécanisme suscite également quelques problèmes du point de vue de la « sécurité ». Théoriquement, si un ou plusieurs participants arrivaient à détenir plus de 51 % de la valeur totale de la chaîne, le poids de son vote surpasserait l'ensemble des autres participants. Un certain nombre d'attaques connues ont également vu le jour concernant ce « consensus » (Martinez, 2018). Il est important de toute fois préciser que certaines sous-implémentations du « PoS »

tendent à corriger ces problèmes en instaurant des mécanismes de punitions ou en introduisant une notion de sélection « aléatoire » à chaque nouvelle validation (Andoni et al., 2019).

Practical Byzantine Fault Tolerance (PBFT)

En informatique, le problème de la tolérance aux pannes (ou aux nœuds défaillants, dans le cadre de la blockchain) dans un système « distribué » et « décentralisé » est généralement illustré par le théorème intitulé « Byzantine Generals Problem » (Lamport et al., 1982). Cette problématique vise à identifier le moyen de faire passer un message au sein d'un réseau distribué, tout en étant conscient que les membres de ce réseau puissent être inatteignables ou malveillants. Le but étant qu'une fois le message passé, les membres ayant autorité sur le réseau puissent prendre la bonne décision, malgré un nombre potentiel d'informations malveillantes reçues (Natoli et al., 2019). Ce concept a inspiré un grand nombre d'algorithmes connus dans le monde informatique, et a également fait l'objet d'un certain nombre d'implémentations en tant que mécanisme de « consensus » au sein des blockchains modernes. Le « PBFT » est un mécanisme de « consensus » qui repose sur ce principe. La particularité de ce mécanisme, contrairement au « PoW » et au « PoS » est que les nœuds ayant autorité pour la validation des blocs (les « généraux ») sont connus à l'avance. Ils sont directement définis au sein de la configuration de la blockchain elle-même. De ce fait, il est important de noter que ce type de « consensus » est particulièrement adapté aux blockchains « privées » et n'est donc pas réellement viable dans une implémentation « publique ». En matière de « sécurité », le « PBFT » accepte un taux de défaillance (ou des nœuds malveillants) inférieur ou égal à un tiers ($\leq 33.\overline{3}$ %) des nœuds (Bach et al., 2018). Si le degré de sécurité semble être nettement inférieur à « PoW » et « PoS » de prime abord, il est important de prendre en compte que nous sommes dans un environnement « privé » et « connu ». Par conséquent, le nombre et l'identité des nœuds participants à la validation des blocs peuvent être maîtrisés, contrairement aux environnements « publics ». En matière d' « évolutivité », le « PBFT » ne semble pas réagir aussi bien que ses prédécesseurs. Induit par le nombre de messages qui transitent entre les nœuds, le temps nécessaire au traitement et à la diffusion des messages augmente de manière exponentielle (des problèmes de performances peuvent être constatés à partir de 20 nœuds (Galas, 2018)). Cependant, tout comme pour les aspects sécuritaires, il est important de comprendre que le nombre de nœuds sera drastiquement plus faible dans un environnement « privé » par rapport à un environnement « public ». Un utilisateur du système n'est pas nécessairement compté comme un « noeud » au sein d'une blockchain « privée ». Le nombre de nœuds (ou de « replicas » de la chaîne) est défini dans la configuration de la blockchain. Finalement, nous pouvons d'ores et déjà statuer que ce type de « consensus » n'influe pas positivement sur la « décentralisation » du système. Les nœuds dépositaires du processus de validations étant connus et sélectionnées en amont de la création de la blockchain, le recours à une ou plusieurs autorités de contrôles centrales est par définition incontournable.

Proof-of-Authority (PoA)

Dans un contexte similaire à celui du « PBFT », le mécanisme de consensus « PoA » préconise l'utilisation d'une liste d'autorités (nœuds) connues à l'avance et ayant le droit de participer au processus de validation d'un bloc. L'ensemble des autorités, défini lors de la configuration de la « blockchain », forment un comité étant le seul garant de la validation des blocs et du « consensus » de la blockchain. À chaque nouveau processus de validation, un membre du comité est sélectionné en tant que « leader » et propose un bloc au restant des membres. Si les membres valident le bloc, il est ajouté à la chaîne. Toute fois, si le bloc est considéré comme étant invalide, le « leader » peut être expulsé du comité et le bloc est donc rejeté. Le principal objectif de cette approche était de créer un mécanisme capable de réduire drastiquement le gaspillage énergétique des consensus tels que « PoW » et était initialement prévu pour des environnements de tests (Natoli et al., 2019). Néanmoins, ce type de consensus tant à gagner en popularité, notamment dans le secteur énergétique, lorsque le système nécessite que l'intégrité et la sécurité des données soient préservées à tout prix (Andoni et al., 2019). En matière de « sécurité », le « PoA » est capable de tolérer un pourcentage de nœuds malveillants supérieur au « PBFT » (< 51 % des nœuds ayant autorité). Toutefois, il est important d'observer en détail les

particularités de chaque implémentation du « PoA » (ex. : « Aura », « Clique ») afin d'assurer que la position de « leader » ne permet pas d'effectuer des validations de blocs malveillantes, au détriment du comité. En termes d'« évolutivité » et de performances, le « PoA » outrepasse les problèmes rencontrés par le « PBFT » grâce au concept de sélection d'un « leader » lors de la validation d'un bloc. Cependant, comme nous l'avons mentionné précédemment, ce gain en performance peut-être parfois obtenu au détriment de l'intégrité des données (Angelis et al., 2017). Concernant les aspects liés à la « décentralisation », le « PoA » se situe dans la même catégorie que le « PBFT » en proposant un mécanisme de « consensus » centralisé pouvant néanmoins, au contraire de « PBFT », être envisagé au sein d'une architecture de blockchain « publique ».

Proof-of-Elapsed-time (PoET)

Ce consensus fait partie d'une nouvelle génération de mécanismes, régulièrement nommé en tant que : « Trusted Execution Environments (TEE) ». La particularité de cette famille de consensus réside dans la méthode avec laquelle elle tente de garantir la « confiance » accordée aux nœuds du système « blockchain ». Les « TEEs », et par transitivité le « PoET » utilisent des algorithmes de sélection aléatoires, basés sur les composants « matériels » de chaque nœud. En effet, ce système est capable de remplacer les preuves de travail (« PoW ») ou les preuves d'enjeux (« PoS ») analysés précédemment, par un processus de sélection basé sur un facteur « aléatoire ». Dans le contexte du « PoET », la blockchain est en capacité d'invoqué une fonction de génération de données aléatoire, directement intégrée au sein du matériel (le processeur de la machine) de chaque nœud du système. Le résultat envoyé par cette fonction permettra au mécanisme « PoET » de déterminer le nœud sélectionné pour la validation du bloc (il se base notamment sur le temps le plus faible, écoulé entre l'initialisation de la fonction et l'obtention de la réponse) (Natoli et al., 2019). Cette technologie est aujourd'hui intégrée et développée par les plus grands fabricants de matériel informatique tels que Intel (Intel Corporation, 2020), AMD (Advanced Micro Devices, Inc, 2020) ou IBM (IBM Corporation, 2020).

La « sécurité » est indéniablement le point fort de cette technologie. Si des attaques restent néanmoins possibles, il apparaît clair que le risque de fraude est fortement réduit et plus complexe qu'au sein du reste des « consensus » analysés (Natoli et al., 2019). En matière d'« évolutivité », le « PoET » semble également être très efficace en se reposant sur des technologies directement embarquées dans le matériel des nœuds du système. Le processus de sélection est ainsi largement plus rapide et moins énergivore que les problèmes à résoudre au sein du mécanisme « PoW ». Néanmoins, si la technologie semble prometteuse en matière de « sécurité » et « évolutivité », elle est intimement liée à la confiance attribuée aux différents constructeurs qui fournissent le matériel agrée. Si le système et le mécanisme de « consensus » et totalement « décentralisé » d'un point de vue architectural, il semble au contraire être « centralisé » sur les plans « logique » et « politique ». Nous ne pouvons par conséquent pas écarter d'éventuelles situations de monopoles ou d'implémentations « frauduleuses », étant dépendantes de l'intégrité et de l'honnêteté des fabricants (Andoni et al., 2019).

Synthèse

Sur la base de notre analyse, nous pouvons à présent dresser un comparatif des différents mécanismes étudiés sur le plan des trois axes identifiés en introduction de cette partie. Nous allons noter les consensus sur une échelle de 1 à 3 pour chaque axe d'analyse identifié (1 étant « non-couvert » et 3 « couvert »).

Tableau 17: Attribution des notes selon les axes d'analyses identifiés

Axes (i)	Poids (w_i)	PoW (c_{i1})	PoS (c_{i2})	PBFT (c_{i3})	PoA (c_{i4})	PoET (c_{i5})
Sécurité	3 (important)	2	2	3[5]	2[6]	2[7]

5 Prise en compte de l'environnement « privé » et donc « maîtrisé » inhérent au « consensus ».
6 Prise en compte des potentiels failles inhérente au concept de « leader » dans certaines implémentations.

Évolutivité	4 (crucial)	1	3	2	3	2[8]
Décentralisation	2 (neutre)	3	3	1	1	1

Nous pouvons maintenant, à l'aide des notes attribuées aux « consensus », calculer le score final obtenu par chacun d'entre eux selon la méthode de « scoring » suivante :

$$S_j = \sum_i w_i c_{ij}$$

Tableau 18: Scores obtenus par les "consensus" selon la méthode de "scoring"

Axes (i)	PoW (c_{i1})	PoS (c_{i2})	PBFT (c_{i3})	PoA (c_{i4})	PoET (c_{i5})
Sécurité	6	6	9	6	6
Évolutivité	4	12	8	12	8
Décentralisation	6	6	2	2	2
Scores (S_j)	16	24	19	20	16

Nous pouvons constater que les mécanismes « PoS », « PoA » et « PBFT » semblent être les plus adaptés à notre cas d'utilisation. Néanmoins, si l'on prend en compte le caractère « privé » de notre implémentation, il semblerait que le consensus « PoS » ne soit pas adapté à ce genre d'implémentations. De ce fait, nous privilégierons les mécanismes « PBFT » et « PoA » lors de la sélection de la technologie « Blockchain ».

D Smart contracts

Le « smart contract » (contrat intelligent) fait partie des critères indispensables à la sélection d'une technologie « blockchain » adéquate avec nos besoins. Son implémentation au sein d'un système « blockchain » offre un panel de fonctionnalités qui peut être vital au bon fonctionnement de l'écosystème que l'on souhaite mettre en place. Nous pouvons le définir de la manière suivante :

> *« Un contrat intelligent est une portion de code informatique qui s'exécute au sein de la blockchain pour faciliter, exécuter et faire respecter les termes d'un accord. L'objectif principal d'un contrat intelligent est d'exécuter automatiquement les termes d'un accord une fois les conditions spécifiées remplies. (Alharby & Moorsel, 2017) »*

Nous pouvons percevoir le « smart contract » comme un « contrat » numérique, qui lie deux ou plusieurs membres d'un même réseau « blockchain » en exécutant une ou plusieurs opérations. Il est généralement déclenché lors de la soumission d'une transaction au sein de la « blockchain ». Nous pouvons comparer le « smart contract » au système de « procédures stockées » existant au sein des bases de données traditionnelles. La logique « métier » et les opérations déclenchées lors de l'exécution d'un « smart contract » dépendent complètement du contexte de la « blockchain ». En effet, si cette fonctionnalité est très souvent associée au processus d'échange de cryptomonnaie, elle peut également être complètement dissociée de ce type d'opérations.

7 Prise en compte de la dépendance instaurées avec les fabricants et l'incapacité de corriger les éventuelles failles sans leurs intervention.

8 Prise en compte de l'environnement « matériel » nécessaire à l'implémentation du réseau.

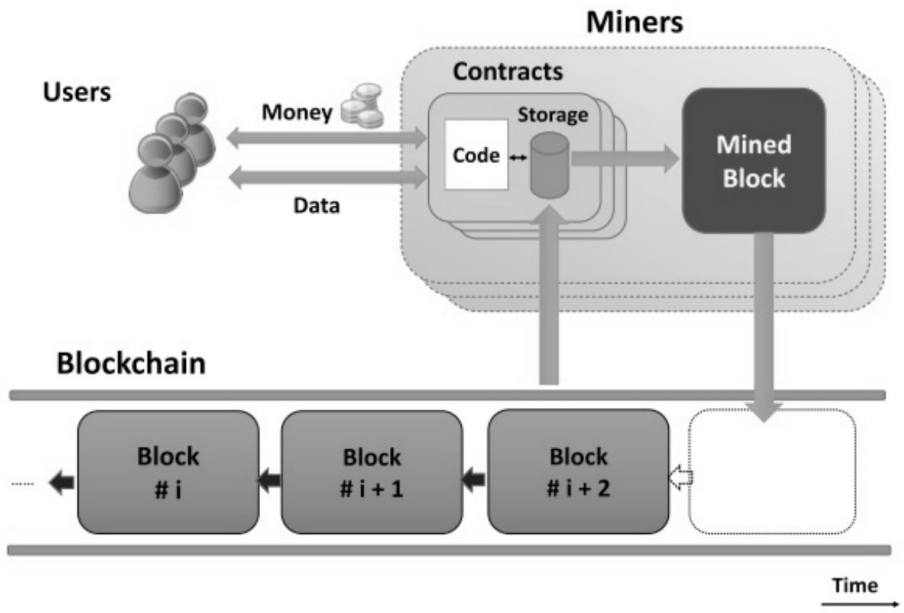


Figure 20: Fonctionnement d'un "smart contract" au sein de la "blockchain" (Alharby & Moorsel, 2017)

Il est important de noter que dans la plupart des blockchains actuelles, le déploiement d'un « smart contract » au sein du système est irréversible. Une fois stocké dans la « blockchain », il ne peut plus être supprimé ou modifié par le créateur (Alharby & Moorsel, 2017). La version du « smart contract » déployé restera donc définitivement stockée au sein de la « blockchain ». Ce comportement nous permet d'affirmer que le processus de déploiement d'un « smart contract » doit être méticuleusement organisé. Il est également judicieux de déployer le « smart contract » dans un environnement de « test » avant de le mettre à disposition des utilisateurs finaux (il existe aujourd'hui des méthodes permettant de mettre à jour les « smart contracts » en mettant en place un système de « versions » (Odisi, 2020)).

Nous n'allons pas explorer en profondeur le fonctionnement des différents types de « smart contract » existant sur le marché durant ce travail. Il existe aujourd'hui de nombreux travaux de recherches qui se focalisent sur ce composant, faisant partie à part entière des systèmes de blockchains actuelles. À l'instar des mécanismes de « consensus », les « smart contract » font également l'objet d'attaques et d'utilisation frauduleuses (ConsenSys Diligence, 2020). Il est donc primordial de prendre en compte ces facteurs lors du déploiement d'un système productif afin d'adopter les meilleures pratiques possible en matière de construction de « smart contracts ».

Dans le cadre de notre implémentation et afin de rendre notre système viable, nous devons nous assurer que la technologie « blockchain » choisie supporte cette fonctionnalité. La possibilité de déployer des « smart contracts » fait partie des conditions-cadres du succès de notre système. Nous allons utiliser cette fonctionnalité afin d'ajouter la notion de « balance » au sein de notre système. Nous voulons que lorsque l'utilisateur du système utilise une borne de rechargement, le nombre de kWh consommés soit automatiquement ajouté à la transaction afin de calculer le montant à payer pour cette dernière. Le montant sera ensuite directement répercuté sur la « balance » de l'utilisateur.

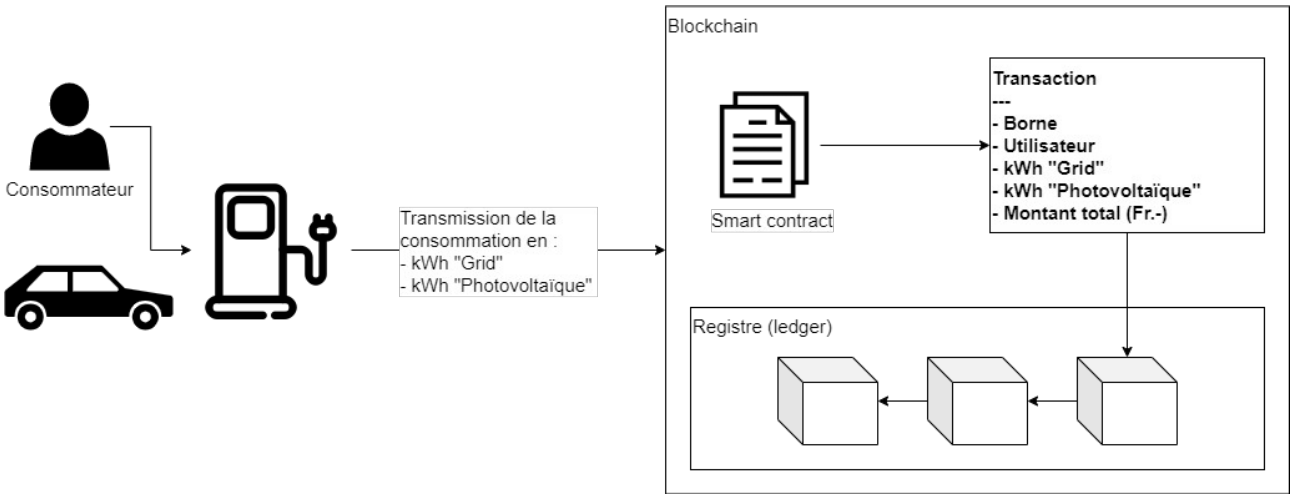


Figure 21: Utilisation des "smart contract" au sein de notre système

Dans notre système, le « smart contract » sera déclenché lorsque le consommateur finalisera le processus de rechargement de son véhicule. La borne enverra ensuite le nombre de « kWh » consommés lors du rechargement au système « blockchain », qui déclenchera automatiquement le « smart contract » afin de calculer le montant total de la transaction. Les opérations devant être réalisées par le « smart contract » nous semblent être à priori relativement simples. Il n'est donc pas nécessaire de prendre en compte la couverture fonctionnelle offerte par chaque système de « smart contract » lors de notre sélection de la technologie.

Nous pouvons donc conclure que dans le cadre de notre implémentation, il nous est nécessaire de garantir que la « blockchain » sélectionnée implémente la fonctionnalité des « smart contracts » afin que nous puissions l'exploiter lors de la validation d'un processus de rechargement.

4.2.2 Technologies retenues

Les processus et les critères de sélection étant pleinement définis, nous pouvons maintenant construire notre comparatif des technologies sélectionnées au commencement de ce chapitre. Les informations récoltées concernant chacune des technologies proviennent directement de la documentation officielle des plateformes. Si l'une des informations n'est pas disponible au sein de la documentation, nous tenterons de la retrouver au sein de sources externes ou nous symboliserons l'absence d'information par un « trait d'union »

A Synthèse et classification des plateformes

Plateforme/ critère	Score	Architecture	Permissions	Mécanismes de « consensus »	Support des « smart contract »	Licence	Prix	Popularité (GitHub)
Ethereum	6	Public	Non	PoW	Oui	LGPL-3.0	Gratuit	25.4K
Hyperledger	6	Privé	Oui	PBFT	Oui	Apache License-2.0	Gratuit	9.7K
MultiChain	6	Privé	Oui	PBFT	Limité (smart filters)	GPL-3.0	Gratuit (community édition) 25'000$ par an (entreprise édition)	478
LiteCoin	5	Public	Non	PoW	Non	MIT License	Gratuit	3.4K
Interbit	4	Public	Non	-	-	MIT License	Gratuit	23
Energy Web	4	Public	Non	PoA	Oui	GPL-3.0	-	-
Tendermint-Cosmos	4	Réseau de blockchain	Oui	Tendermint BFT	Oui	Apache License-2.0	Gratuit	1.6K
KSI	4	Privé	Oui	-	Non	Apache License-2.0	Gratuit	14
Qtum	4	Public	Non	PoS	Oui	MIT License	Gratuit	1.1K
Ripple	2	Public	Oui	Propriétaire	Oui	Personnalisé	Gratuit	3.4K

La synthèse réalisée ci-dessus nous permet d'identifier rapidement la seule plateforme ayant rassemblé l'ensemble des critères que nous avons définis au cours de ce chapitre : « *Hyperledger* ». En effet, elle dispose d'un mécanisme de permission et supporte l'implémentation des « smart contracts ». De plus, le mécanisme de « consensus » utilisé par la plateforme correspond à l'un des deux mécanismes retenus par notre processus de sélection (PBFT). Elle bénéficie également d'une popularité élevée et à l'avantage d'être sous licence « Apache », ce qui la rend parfaitement exploitable dans le cadre de notre implémentation « Proof-of-Concept ».

4.3 Implémentation du « proof-of-concept »

Faisant suite au déroulement du processus de sélection d'une plateforme adéquate avec les besoins de notre système, nous avons sélectionné la plateforme « Hyperledger » comme étant la « blockchain » la plus adaptée à notre environnement. Il faut savoir que le terme « Hyperledger » désigne en réalité un projet collaboratif supporté par la « Linux Foundation » qui vise à créer et promouvoir des solutions « blockchain » qui soient en adéquation avec les besoins de l'industrie. Elle regroupe un certain nombre d'implémentations de la « blockchain », toutes destinées à couvrir un besoin particulier.

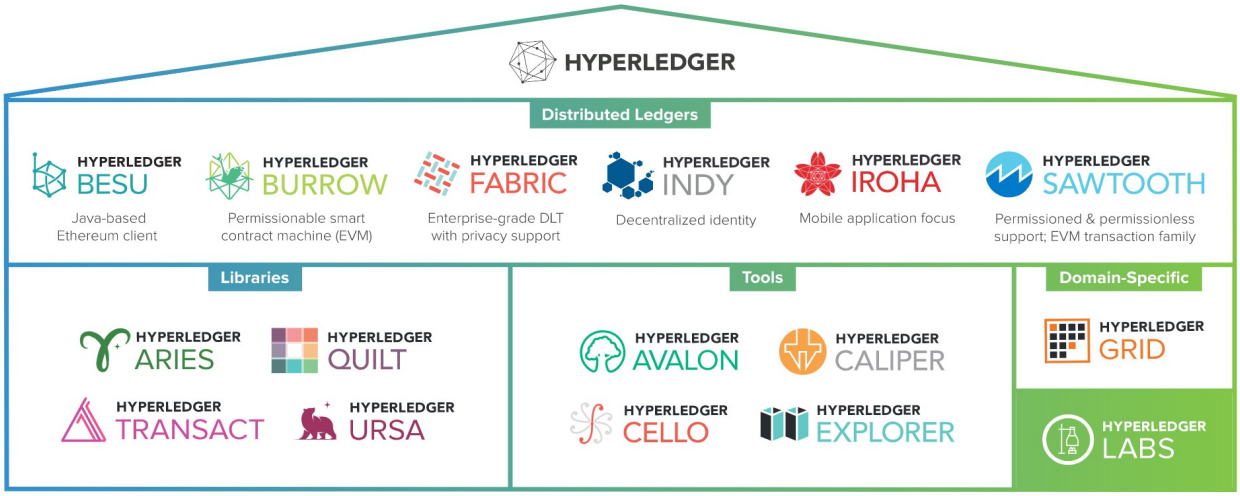


Figure 22: Présentation des produits proposés par "Hyperledger"

Historiquement, la mention de la plateforme « Hyperledger » au sein de la littérature spécialisée désigne en réalité l'implémentation « Hyperledger Fabric ». Cette implémentation de la « blockchain » est la première l'implémentation et la plus populaire du projet. Nous utiliserons donc la plateforme « Hyperledger Fabric » pour la mise en place de notre « Proof-of-Concept ».

Nous avons dans un premier temps pris connaissance de concepts fondamentaux liés à cette technologie afin d'en entrevoir les possibilités et de juger du niveau de complexité à sa mise en place. Nous avons commencer par la mise en place d'un système de test simple au sein de notre environnement machine (PC portable « Windows »). Lors de cette phase, nous avons rencontré de nombreuses difficultés qui nous empêché de rendre notre test fonctionnel au sein de notre environnement de départ (ex. : problèmes de déploiement, problèmes de dépendances liés au système « docker »). Suite à cet échec, nous avons décidé d'adopter une méthodologie différente afin d'accélérer la prise en main de la technologie et rattraper le temps perdu dans notre implémentation de départ. Pour ce faire, nous avons cherché sur internet des exemples d'implémentations fonctionnels se rapprochant de notre cas d'utilisation. Lors de cette recherche, nous n'avons trouvé aucune implémentation publique et libre de droits permettant de servir de modèle pour notre implémentation. Dans le cadre de notre formation, nous avons eu l'occasion d'assister au « Hyperledger Global Forum 2018 » à Bâle. Par le biais de notre inscription, nous avons eu accès à l'ensemble des présentations et conférences (au format .pdf) qui se sont tenues lors de cette semaine de forum. Nous avons donc recherché les potentiels « workshop » ayant lieu cette semaine et utilisant la technologie « Hyperledger Fabric » comme exemple d'implémentation. Notre recherche nous a permis d'obtenir une présentation intitulée « Getting Started with Hyperledger Fabric using Golang » et présentée par la société « ChainHero » (la présentation se trouve en annexe de ce document). Elle décrit le fonctionnement de la technologie et implémente un système basé sur

« Hyperledger Fabric » qui illustre un modèle basé sur le principe de consommation et libération de ressources au sein de la « blockchain » (Chabert, 2018). Le système mis en place dans le cadre de ce « workshop » correspond au modèle que nous souhaitons implémenter et se trouve être sous licence « Apache 2.0 ». De ce fait, nous avons utilisé ce système comme base pour notre implémentation « Proof-of-Concept ». Le code contenant l'implémentation de base du système présenté par « ChainHero » est disponible gratuitement sur la plateforme « GitHub » à l'adresse suivante : « *https://github.com/chainHero/resource-manager* »

4.3.1 Présentation du système

Dans le cadre de ce travail, nous avons été en mesure d'acquérir et déployé le système proposé par « ChainHero » et modifiant certaines spécificités afin de le rendre compatible avec les attentes de notre système. Le système se présente sous la forme suivante

A Authentification

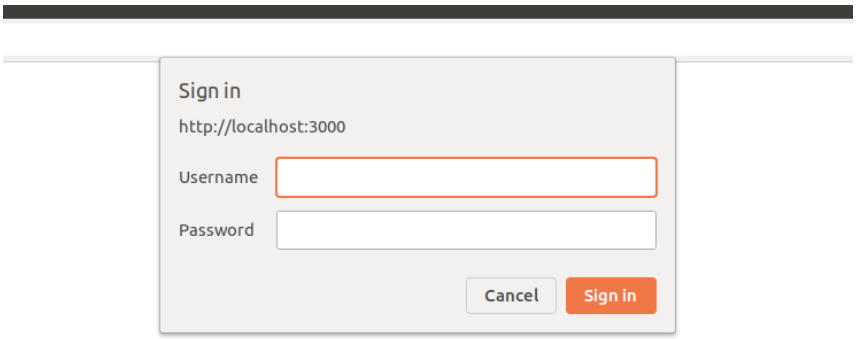


Figure 23: Authentification au sein de l'application

Lors de notre arrivée au sein de l'application, le navigateur nous demande de saisir un nom d'utilisateur et un mots de passe afin d'accéder au système. Comme définis lors de présentation de notre concept, le système dispose de deux niveaux d'accès distincts : le consommateur et l'administrateur. Dans notre système, nous avons créé les comptes suivants :

- Nom d'utilisateur : *admin1* | Mot de passe : *password* | Rôle : *administrateur*
- Nom d'utilisateur : *consumer1* | Mot de passe : *password* | Rôle : *consommateur*
- Nom d'utilisateur : *consumer2* | Mot de passe : *password* | Rôle : *consommateur*

Ces comptes nous permettent d'accéder aux différentes fonctionnalités mises à disposition par le système.

B Accueil

Figure 24: Page d'acceuil de l'application

La page d'accueil permet de visualiser l'état des ressources du système. Nous pouvons dans cet exemple voir que le système dispose de quatre ressources (bornes) et qu'elles sont toutes disponibles à l'heure actuelle. L'application dispose d'un menu de navigation situé sur le haut de l'écran qui permet à l'utilisateur de naviguer au sein de sections auxquelles il a accès.

C Liste des ressources

La liste des ressources offre une vue personnalisée en fonction du rôle dont dispose l'utilisateur au sein du système. En effet, un consommateur doit pouvoir accéder à la liste des ressources afin de sélectionner une borne de chargement et commencer le processus de recherche de son véhicule.

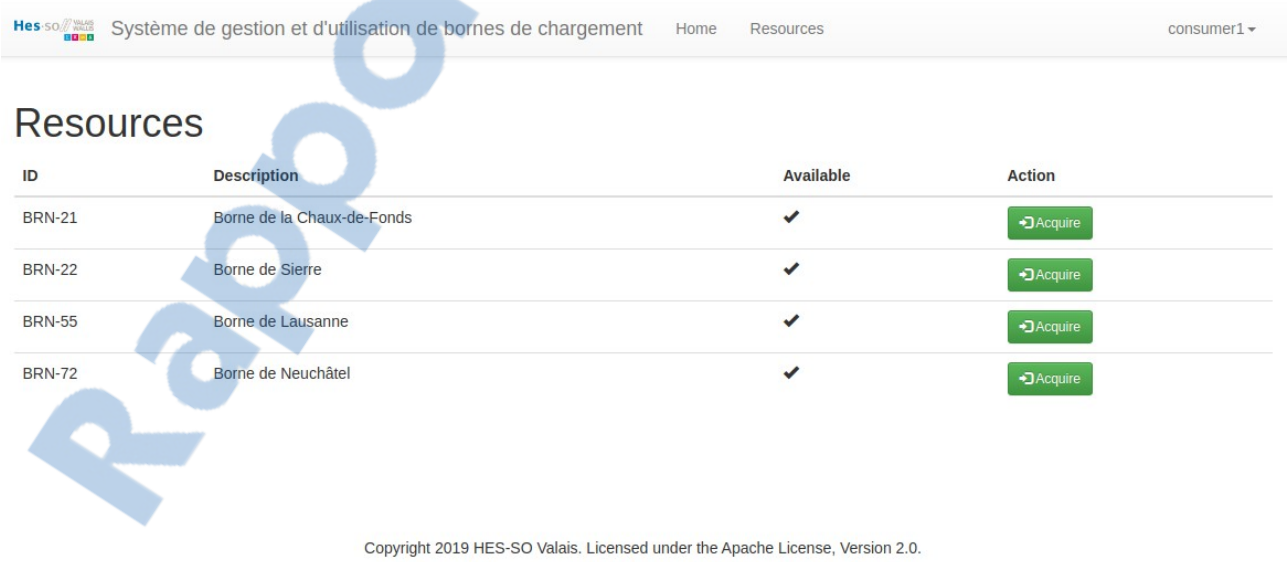


Figure 25: Liste des ressources selon la perspective du consommateur

Dans la perspective de l'administrateur du système, il doit pouvoir accéder à la liste des ressources afin de visualiser l'état des bornes de chargement et gérer leur cycle de vie.

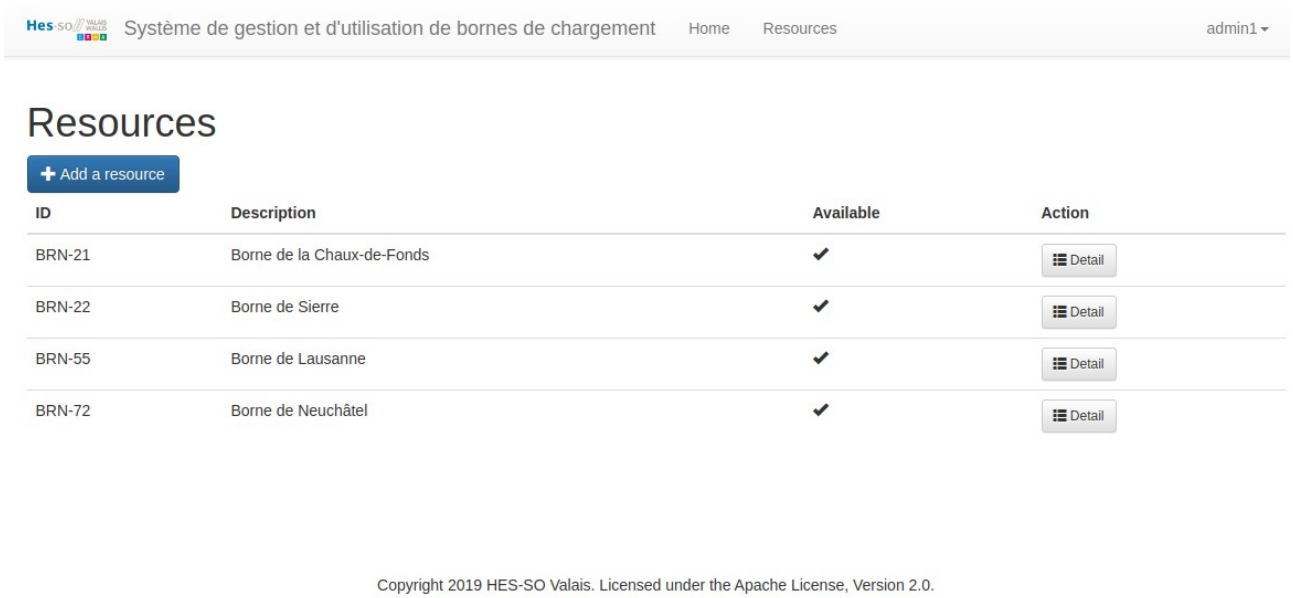


Figure 26: Liste des ressources selon la perspective de l'administrateur

D Détails d'une ressource

En tant qu'administrateur, nous avons la capacité de visualiser plus en détail les ressources du système afin d'inspecter les transactions relatives à une borne de chargement spécifique. Dans l'implémentation actuelle, nous avons la possibilité de voir un historique des transactions faites pour une borne données et contenant les informations suivantes : date de la transaction ; statut de la borne et le numéro de la transaction au sein du système.

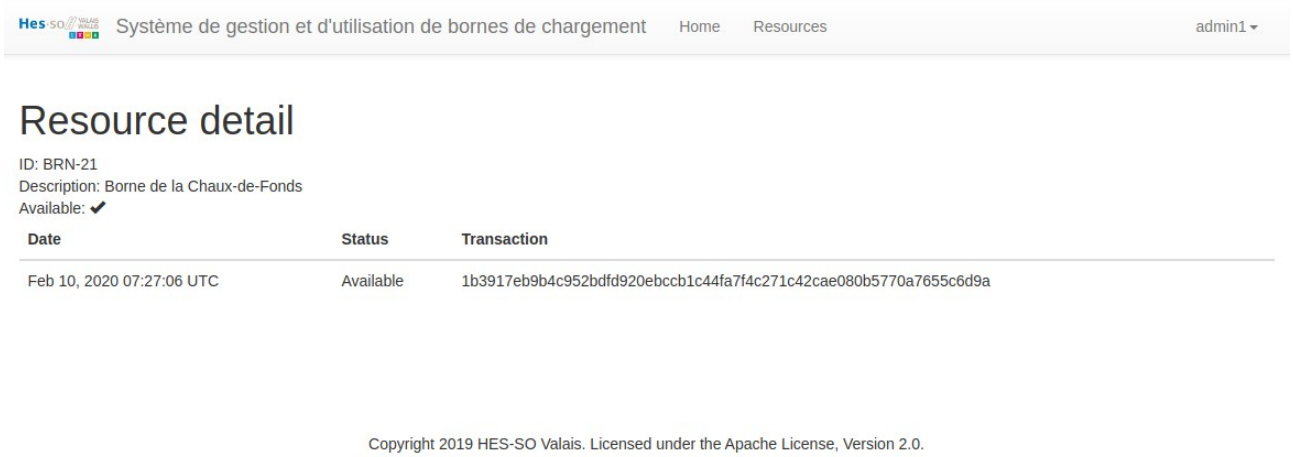


Figure 27: Visualisation détaillé d'une borne de chargement selon la perspective de l'administrateur

E Ajout d'une ressource

Finalement, l'administrateur à la possibilité d'ajouter de nouvelles ressources au sein du système afin qu'elles soient visibles et utilisable par les consommateurs.

Figure 28: Ajout d'une ressource selon la perspective de l'administrateur

Les éléments présentés ci-dessus représentent l'état de notre implémentation « Proof-of-Concept » au moment du rendu de cette étude.

4.3.2 Résultats obtenus et difficultés rencontrées

Lors de notre implémentation, nous avons rencontré plusieurs difficultés qui ne nous ont pas permis d'atteindre l'objectif fixé en introduction de ce chapitre. En effet, lors du déploiement de la solution implémentée par « ChainHero », nous avons été confrontées à des erreurs de compilations provenant de la configuration interne de « Hyperledger Fabric » qui nous ont bloqués dans l'adaptation du modèle de base vers le modèle que nous avions défini pour cette implémentation. Nous avons tenté de résoudre les diverses erreurs rencontrées afin de disposer au minimum d'un système fonctionnel et exécutable. Nous sommes parvenus à atteindre cet objectif en adressant les problèmes suivants :

- Erreurs de compilations liées au mauvais référencement du langage « GO » au sein du « PATH » du système Linux hôte.
- Erreurs de compilations liées à une version de « docker-compose » inadéquate avec l'environnement du projet
- Erreur de compilations internes au déploiement du réseau « Hyperledger Fabric », nous avons mis à jour la plateforme et ses différentes dépendances vers la dernière version disponible.

L'identification et la résolution de ces différents problèmes ont été un frein conséquent à l'implémentation du modèle attendu. De ce fait, nous avons gardé le modèle de base implémenté par la société « ChainHero » en supprimant des notions peu pertinentes dans le cadre de notre système. Nous avons également légèrement adapté les pages afin qu'elles soient aux couleurs de l'institution « HES-SO ». Nous clôturons ainsi la phase d'analyse et développement sur la présentation des résultats obtenus.

5 Synthèses et conclusion

Ce chapitre a pour fonction de clôturer notre étude en faisant une synthèse de l'ensemble des informations récoltées au sein de ce travail. Les analyses et recherches effectuées lors des chapitres précédents vont nous permettre de formuler des conclusions et recommandations aux acteurs touchées par la thématique abordée. Nous pouvons rappeler ici notre question de recherche principale, qui était la suivante :

> *Quels sont les impacts et enjeux de la technologie "blockchain" dans le contexte de la mobilité électrique ?*

Tout au long de ce travail, nous avons exploré et analysé le fonctionnement de la technologie « blockchain » afin d'en extraire ses caractéristiques principales. Nous avons notamment défini que le concept de « blockchain » se rapportait à un nouveau type de base de données « distribuée » et « décentralisée », qui organisait le stockage de ses données sous forme de transactions. Le caractère « distribué » et « décentralisé » du réseau permet notamment de garantir une immuabilité des transactions dans le temps, ce qui fait de la « blockchain » un réseau fiable par nature. Nous avons pu identifier un certain nombre d'apports et d'avantages offert par cette technologie en comparaison avec les systèmes traditionnels. Il a été défini que la « blockchain » implémente des mécanismes qui augmentent significativement le niveau de sécurité et de confiance que l'on peut avoir dans le système. Par transitivité, cette confiance accrue du système permet à ses acteurs d'interagir les uns avec les autres sans avoir à se connaître ou à se faire confiance mutuellement. En effet, le système agit de lui-même, et de manière autonome (sans avoir recours à un tiers de confiance), en tant qu'autorité de contrôle. Néanmoins, nous avons également pu voir que cette technologie est aujourd'hui en constante évolution et encore en phase de maturation. Nous avons identifié plusieurs problématiques soulevées par les premières implémentations de cette technologie, notamment en matière de performance et de consommation énergétique (principalement causés par les mécanismes de « consensus »). De plus, à l'heure où les questions concernant la protection des données se font grandissantes, la technologie « blockchain » inquiète certains secteurs par la transparence et le caractère immuable de son fonctionnement (Tableau 6: Synthèse des apports et des limites de la technologie "blockchain" dans un système). Ces problématiques ont aujourd'hui pour effet de tempérer l'engouement de l'industrie pour la « blockchain ». Néanmoins, il ne fait aucun doute que le potentiel de la technologie est réel et ces problèmes sont aujourd'hui déjà adressés par les implémentations modernes du concept. Ces éléments nous ont également permis de répondre à notre première question de recherche (*RQ1)*.

La compréhension des concepts cités ci-dessus nous a permis de parcourir la littérature à la recherche d'exemples d'implémentation de la « blockchain » au sein du secteur énergétique suisse, et plus particulièrement dans le cadre de la mobilité électrique. Ces exemples nous ont permis de confirmer la pertinence de notre problématique de départ, en démontrant l'intérêt déjà existant des acteurs du secteur énergétique pour cette technologie. Nous avons notamment pu voir que la technologie « blockchain » était aujourd'hui appliquée à des fins bien différentes au sein de ce même secteur. Nous avons identifié des initiatives visant à créer des communautés « énergétiques », tels que « HivePower », « Energy Web » ou encore « Prosume ». Nous avons également vu d'autres champs d'applications, tels que celui qui nous intéresse, implémenté par « Energie Wasser Bern » en collaboration avec « Swisspower ». Dans ce projet pilote, la société énergétique bernoise teste un système permettant la recharge des véhicules électriques via une infrastructure « blockchain ». Ce projet est sans aucun celui qui se rapproche le plus de notre problématique de départ et qui démontre la pertinence et la faisabilité de notre système. Les exemples précédemment cités nous ont permis de définir la pertinence de la technologie dans le cadre de la mobilité électrique et de répondre à notre deuxième question de recherche (*RQ2*).

La revue de la littérature nous a permis d'explorer l'ensemble des concepts théoriques abordés lors de cette étude. Nous avons ensuite abordé la partie d'analyse et de développement en présentant le système que nous souhaitions mettre en place afin d'en démontrer le fonctionnement (Figure 14: Fonctionnement de notre système "Proof-of-Concept"). Le système proposé visait à démontrer la possibilité d'utiliser la technologie « blockchain » comme plateforme de support aux transactions engendrées par le rechargement des véhicules électriques. Le système présenté tient compte de l'asymétrie, en matière de fonctionnalités et d'accès aux données, existant entre les deux principaux acteurs du processus que sont le « consommateur » et « administrateur » du système. Afin de mettre en place ce système, nous avons dû procéder à une revue des solutions existantes sur le marché et définir un protocole de sélection qui tient compte des éléments indispensables lors de la sélection d'une plateforme basée sur la « blockchain ». Ce protocole tient compte des éléments suivant : *l'architecture et les permissions du réseau; la nature et le stockage des données; le mécanisme de « consensus »; le support des « smart contracts »; la licence et les conditions d'utilisation; le prix et la popularité ou support de la communauté*. Ces notions, compte tenu de la nature de la technologie et des éléments identifiés au sein de la littérature, nous semblent être les critères essentiels à la sélection d'une plateforme qui soit en adéquation avec les besoins d'un système d'information fiable et évolutif. Ces critères apportent également une réponse directe à notre troisième question de recherche (*RQ3*). Finalement, le processus de sélection nous a menés à choisir la plateforme « Hyperledger Fabric » en tant que plateforme de développement pour notre implémentation « Proof-of-Concept ». Les résultats obtenus suite à l'implémentation du système n'ont pas couvert l'ensemble des attentent fixé au début de cette étude. En effet, il s'est avéré que la technologie nécessite un niveau de compétences et de compréhension du système relativement élevé. De ce fait, nous avons été en mesure de récupérer et mettre en œuvre le système présenté par la société « ChainHero » lors du « Hyperledger Global Forum » qui s'est déroulé dans le courant de l'année 2018 à Bâle (voir annexe Erreur : source de la référence non trouvée-Erreur : source de la référence non trouvée). Le système de base, présenté lors du « workshop », posait les fondations nécessaires à la mise en place et à la configuration « Hyperledger Fabric » et implémentait un système basé sur la consommation et l'administration de ressources au sein de la « blockchain ». La pertinence du modèle et la proximité affichée avec les objectifs que l'on souhaitait atteindre nous ont convaincus de baser notre implémentation sur ce modèle. Nous avons néanmoins rencontré plusieurs difficultés lors de la mise en place de système. Plusieurs problèmes de « compilations », pour la plupart liés à la version de « Hyperledger Fabric » utilisés à l'époque, nous ont freiné dans l'implémentation de notre système. À ce jour et au moment du rendu de cette thèse, nous avons été en mesure de rendre le prototype fonctionnel et exploitable, au détriment de toutes les notions que nous souhaitions initialement intégrer (ex. : kWh consommés, source de la consommation, etc.). Cependant, le prototype couvre les notions essentielles du système attendu, à savoir la mise en place d'une infrastructure « blockchain » dotée de permissions et capable de supporter la structure de données attendue. Nous sommes donc en mesure d'analyser l'impact de la technologie « blockchain » dans le contexte d'un système chargement des véhicules électriques.

5.1 La « Blockchain » dans le système implémenté

En tant que système, nous pouvons clairement définir que l'implémentation de la technologie « blockchain » au sein de notre « POC » a été un succès. En effet, la technologie semble être capable de supporter les structures de données relationnelles classiques et permet d'inscrire, de manière immuable et permanente, l'ensemble des transactions produites par le processus de rechargement d'un véhicule électrique. Nous pouvons définir que la technologie « blockchain » est compatible avec notre cas d'utilisation, et donc avec des potentielles implémentations dans le cadre de la mobilité électrique. L'exemple du projet pilote porté par « Energy Wasser Bern » va également dans ce sens en présentant une implémentation concrète de ce type d'applications. Cependant, dans le cadre de notre implémentation, nous dénotons un certain nombre de points qui doivent être pris en compte lors de futures implémentations. Par nature, la technologie « blockchain » porte des promesses telles que la transparence du système, l'absence de tiers de confiance et l'immuabilité des données. Or, nous

sommes forcés de constater que dans notre architecture (réseau « privé » à permissions), ces promesses ou objectifs ne sont pas atteints. La nature des « blockchains » privées, ou orientées application d'entreprises, induit qu'il existe plusieurs « versions » du registre de données, en fonction des permissions accordées aux participants. En réalité, un réseau « privé » est un réseau composé de sous-réseaux qui disposent de leurs propres logiques (ex. : registres, « smart contracts », participants). Au sein de la plateforme « Hyperledger Fabric », ces sous-réseaux sont cités comme étant des « Peers ».

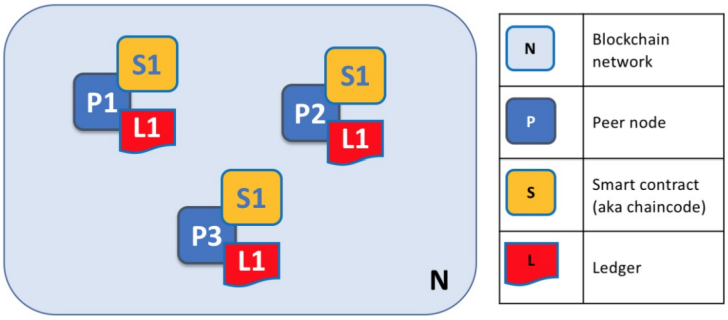


Figure 29: Fonctionnement du réseau "Hyperledger Fabric" (The Linux Foundation, 2019b)

Si ce mode de fonctionnement semble apporter une plus grande flexibilité au niveau de la configuration et de l'évolutivité du réseau, il questionne toute foi sur l'absence des principes fondamentaux historiquement associés à la technologie « blockchain » (ex. : transparence, absence de tiers de confiance, autonomie du réseau). Yves Caseau et Serge Soudoplatoff (2016) considèrent que si les cinq conditions majeures, nécessaires à l'implémentation d'un système « blockchain » ne sont pas réunies (à savoir la confiance distribuée ; un système transactionnel fiable; la validation des données par une large communauté ; l'absence de tiers de confiance ; l'exécution autonome de protocole complexe), alors la « blockchain » peut être remplacée par un système dédié traditionnel, capable de réaliser les mêmes opérations à moindres coûts. Dans le cadre de notre implémentation, nous constatons effectivement que nous aurions pu atteindre le même résultat sans avoir recours à la technologie « blockchain ». Nous justifions ce constat sur la base des critères présentés ci-dessous.

Tableau 19: Critères d'analyses jugeant la pertinence de la "blockchain" au sein de notre système

Critère	Description
Absence de transparence	Le consommateur ne voit que les transactions qui le concernent (ce qui fait sens d'un point de vue « métier » dès lors qu'un utilisateur est formellement identifié, mais semble être contradictoire dans le contexte de la « blockchain »). Ce genre de systèmes à permissions est facilement réalisable à l'aide d'un SGBD traditionnel.
Nécessité d'un tiers de confiance	L'administrateur du réseau (ou fournisseur énergétique) est dans le contexte de notre implémentation le seul dépositaire des autorisations du système. Par conséquent, le mécanisme de « consensus », fondamentale dans le contexte de la « blockchain » ne fait aucun sens dans ce cas précis. Nous sommes donc en présence d'un système complètement politiquement « centralisé », implémentable à moindres coûts dans le contexte d'un système de base de données traditionnel.

Absence de « distribution » et de « décentralisation »	D'un point logique et architectural, notre système se trouve être complètement « centralisé » sur les deux plans. En effet, la manipulation de la « blockchain » étant réalisée par intermédiaire d'une interface web dédiée, le consommateur ne se trouve jamais en possession d'une copie de la chaîne en local. Nous nous retrouvons donc dans une architecture classique à un nœud avec un administrateur.

Pour ces raisons, nous jugeons l'utilisation de « blockchain » démesurée dans le cadre du système que nous avons mis en place. Nous remettons principalement en question le modèle proposé par les blockchains de type « privé » *lorsque le système est régulé par une seule entité physique ou morale*. Dans ce contexte, les coûts et la complexité liés à la mise en place d'un système « blockchain » nous semblent trop élevés par rapport aux avantages et fonctionnalités du système. L'utilisation d'une « blockchain » de type « privé » nous semble pertinente *lorsque le système abrite plusieurs autorités devant collaborer sous forme de « consortium » afin d'administrer le réseau*. Pour cette raison, nous pensons que la technologie est néanmoins pertinente dans le cadre d'une implémentation complète du processus lié à la mobilité électrique. En effet, contrairement à notre implémentation, le système proposé par la « Energy Web Fondation » repose sur un « consortium » d'acteurs du secteur énergétique faisant autorité sur le réseau. Dans ce cadre, la « blockchain » et les mécanismes de « consensus » qu'elle implémente apportent une réelle plus-valu au fonctionnement du système.

Nous pouvons clôturer cette partie en affirmant que la technologie « blockchain » à un réel potentiel dans le cadre de l'implémentation d'un système informatique dédiée au rechargement des véhicules électriques. Néanmoins, le succès de cette implémentation nécessite un certain nombre de conditions-cadres afin d'être pertinente et en accord avec les valeurs portées par la technologie.

Tableau 20: Conditions-cadres nécessaires à l'adoption de la "blockchain"

Condition	Description
Besoin de « distribution » et de « décentralisation »	Un système basé sur la « blockchain » doit impérativement intégrer ces deux paradigmes. Ils peuvent être intégrés du côté des consommateurs ou des régulateurs du réseau. Ces notions introduisent une notion de « partage de l'information » qui est critique lorsqu'on évalue la pertinence de cette technologie.
Besoin de « confiance »	Un besoin de confiance, d'immuabilité et d'historisation des transactions est nécessaire pour considérer l'adoption de la technologie « blockchain » au sein d'un système. Ces notions la distinguent particulièrement des systèmes traditionnels et justifient sa présence en tant que pierre angulaire d'un système.
Besoin de « consensus »	L'introduction de la « blockchain » au sein d'un système composé d'une seule entité responsable de l'autorité est inutile. Cette technologie est fondamentalement portée par le besoin de « distribution » et d'obtention d'un « consensus » entre les différentes parties prenantes du réseau.

Ce constat vient répondre de manière directe à notre quatrième et dernière question de recherche (*RQ4*).

5.2 Potentiel de la technologie dans le secteur énergétiques

Le travail réalisé lors de cette étude nous a permis d'identifier et comprendre les problématiques majeurs adressé par la technologie « blockchain ». Nous pouvons aisément dire que ces problématiques sont aujourd'hui rencontrées au sein d'une multitude de secteurs bien distincts. En effet, les processus liés au

traitement de l'information représentent aujourd'hui un défis et un enjeux majeurs à la pérennité des système d'informations. Le secteur énergétique ne fait pas exception à cette règle et peut grandement bénéficier des concepts apporté par la « blockchain » afin d'optimiser ou totalement transformé certain processus ou modèles actuelles. Au-delà du cadre de la mobilité électrique (que nous venons de présenter), nous pouvons entrevoir un certain nombre de domaines dans lesquels la « blockchain » peut intervenir dans ce secteur. Andoni et al. (2019) identifient les secteurs pouvant être potentiellement touchées par l'avenénement de la « blockchain » de la manière suivante.

Tableau 21: Impacts de la technologie "blockchain" au sein du secteur énergétique (Andoni et al., 2019)

Secteur	Description
Facturation	La « blockchain », les « smart contracts » et les compteurs intelligents peuvent servir de base à la réalisation d'un système de facturation entièrement automatisée pour les consommateurs. Les sociétés de services pourraient bénéficier du potentiel des micropaiements énergétiques, des solutions de paiement à l'utilisation ou des plateformes de paiement pour les compteurs prépayés
Ventes et « marketing »	Les pratiques de vente peuvent changer en fonction du profil énergétique des consommateurs, des préférences individuelles et des préoccupations environnementales. En combinaison avec des techniques d'intelligence artificielle telles que le « Machine Learning », la « blockchain » serait en mesure d'identifier les modèles énergétiques des consommateurs et donc permettre la fourniture de services personnalisés et à forte valeur ajoutée.
Marchés et commerce	L'avènement des plateformes de « trading (échanges) » basées sur la blockchain peuvent totalement bouleverser les processus commerciaux établis. Les transactions de matières premières et la gestion des risques font partie des secteurs pouvant être impacté positivement par cette technologie
Réseaux intelligents et transfert de données	La « blockchain » peut potentiellement être utilisées en tant que plateforme pour la communication entre les appareils intelligents (compteurs intelligents, capteurs, équipements de surveillance du réseau, système de surveillance de la consommation des bâtiments) ainsi que pour la transmission ou le stockage de données. En plus de fournir un transfert de données sécurisé, la « blockchain » peut contribuer à la normalisation des données produites au sein du réseau.
Automatisation	Le caractère « autonome » de la « blockchain » peut participer à la gestion des réseaux « domestiques (micro-grid) » en simplifiant les échangent énergétique au sein du réseau. Ce mode de fonctionnement peut grandement encourager les consommateurs à consommer et produire leurs propres énergie afin d'augmenté la rentabilité et l'efficience du réseau. Une telle pratique pourrait même devenir un source de revenue pour le consommateur (échange ou vente d'énergie sur le réseau).
Gestion des réseaux	La « blockchain » pourrait participer à la gestion des réseaux de consommation décentralisé ou privés en agissant en tant que passerelle de communication entre les différents réseaux, sans avoir à remanier les structures existantes.
Sécurité et identification	La protection des transactions et la sécurité peuvent bénéficier de techniques cryptographiques. La blockchain pourrait protéger la vie privée, la confidentialité des données et la gestion des identités.
Partage des	La « blockchain » pourraient servir de plateforme pour le partage de ressources entre

ressources	plusieurs utilisateurs (ex. : borne de chargement, données, capacité de stockage).
Compétitivité du marché	La visibilité et l'automatisation offerte par les « smart contracts » peuvent significativement simplifier la lisibilité des contracts et favoriser le changement de fournisseur au au sein d'un réseau. Cet apport en compétitivité devrait potentiellement réduire les tarifs du marché
Transparence	Le caractère immuable et transparent de la « blockchain » peut considérablement améliorer les processus d'audit et mises au normes du secteur.

Les impacts présentés ci-dessus nous donnent une indication forte concernant le potentiel de la technologie « blockchain » au sein du secteur énergétique. Elle a le potentiel de transformer un large ensemble de processus établis, en amenant de la normalisation, de la transparence, de l'automatisation et la compétitivité au sein du marché. Le modèle basé sur l'autoconsommation et l'autoproduction d'énergie par les particuliers nous semblent être la prochaine grande transformation du secteur, qui sera indéniablement portés par cette technologie. En effet, le modèle de « prosumer (producer/consumer) » est régulièrement mis en avant dans la littérature scientifique et spécialisées. Lors de sa présentation, Plain (2019) entrevoit même ce modèle comme étant l'une des clés contribuant à l'accessibilité de l'électricité dans les pays en voie de développement, sans impacter négativement l'environnement. L'étude menée par PwC (2016) met également en lumière ce scénario en comparant la structure du marché avant et après l'adoption de la « blockchain »

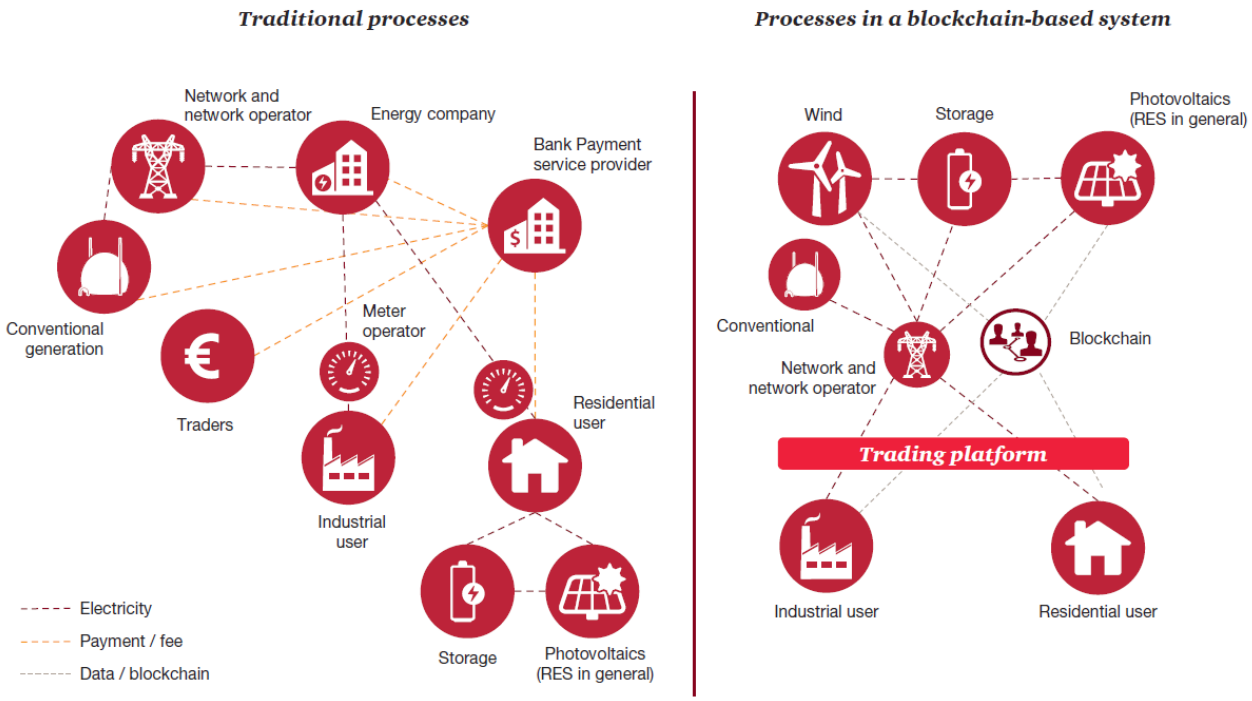


Figure 30: Comparaison de la structure du marché sans et avec la "blockchain" (PwC, 2016)

Nous pouvons constater que la « blockchain » agit comme une véritable plateforme d'échange d'informations (énergie, données) permettant de rendre le marché ouvert et transparent. Dans ce modèle, les consommateurs peuvent se transformer en producteurs et les producteurs se transformer en consommateurs. Si ce changement de paradigme est réalisé en favorisant la transition vers des sources d'énergies renouvelables (ex. : panneaux solaires, éoliens, hydrauliques), il ne fait aucun doute que l'intégration de ce modèle sera l'enjeu majeur de l'adoption de la technologie « blockchain » au sein du secteur énergétique. Si nous avons déjà mis en

lumière les opportunités et les impacts positifs de ce modèle, nous devons également tenir compte des potentiels défis qui accompagneront ce changement.

Tableau 22: Identification des risques liés au changement de modèle (PwC, 2016)

Risques
La centralisation des informations au sein de la « blockchain » interroge sur la gestion des utilisateurs et de leur identité. La perte des accès ou le vol d'identité (de la clé « SSH » dans le contexte d'une blockchain publique) engendrerait une perte complète des données et du contrôle du consommateur.
Coûts de transaction actuellement élevés pour systèmes de blockchain publics (dû au consensus, réglé à l'avenir et dans les blockchains privées)
L'introduction d'une nouvelle technologie, et donc d'un changement, au sein du système pourrait déclencher une réaction de « rejet » de la part du consommateur (peur du changement, manque de maîtrise vis-à-vis du nouveau modèle). La formation et l'information du consommateur sont cruciales pour éviter ce risque.
Un système ayant pour seule autorité le système lui-même (la « blockchain ») interroge sur l'absence d'interlocuteurs en cas de litige ou de panne sur le réseau. Il faudra élaborer des modèles ou définir un comité de régulation afin d'éviter ce genre de problèmes.
Les systèmes de mesures intelligents (« smart meters », « smart devices ») font partie intégrante du modèle « prosumer ». Néanmoins, ces systèmes font partie du monde réel (physique) et sont donc susceptibles d'être corrompus ou compromis afin de procéder à des activités frauduleuses au sein de la « blockchain ». La sécurisation des ces systèmes, d'un point de vue physique et informatique est indispensable pour garantir la viabilité et l'intégrité du système.
Le manque de recul et d'expérience vis-à-vis de la technologie « blockchain » peut être un frein à l'adoption de la technologie ou une source de problèmes lors de son implémentation
Les éventuels problèmes techniques qui peuvent surgir à l'utilisation de système complexe peuvent grandement perturber le fonctionnement du réseau. Ces possibilités doivent être envisagées en amont dans la mesure où elles sont difficiles à prévoir et à identifier (lié au manque d'expérience).
La diversification et la multiplication des réseaux peuvent engendrer des problèmes de normalisation des données (plateformes différentes, niveaux de permissions différents). Dans une optique d'interconnexion des réseaux énergétiques, il sera nécessaire d'établir des standards en matière de protocoles de communication et de formats de données échangées.
L'organisation et la topologie des réseaux seront de plus en plus complexes. Le système doit garantir un au degré de flexibilité afin d'être en mesure d'absorber ce modèle.
Les réglementations et cadres légaux existants aujourd'hui ne prennent pas encore en compte ce nouveau type de technologies. Une analyse approfondie est nécessaire afin de garantir que le système soit en adéquation avec les législations actuelles.

En conclusion de cette partie, nous avons pu démontrer les impacts et enjeux majeurs liés à l'utilisation de la technologie « blockchain » au sein du secteur énergétique. Les facteurs identifiés peuvent servir de recommandation et d'avertissement pour les acteurs du secteur lors de leur processus d'adoption de la technologie « blockchain ». Les analyses présentées ci-dessus permettent également de répondre à notre question de recherche principale, et donc de clôturer notre synthèse.

5.3 Conclusions

Le travail réalisé lors de différentes phases de notre étude nous a permis d'appréhender les concepts, les impacts et les enjeux liés à la technologie « blockchain ». Nous avons pu mesurer ces aspects dans le cadre de la mobilité électrique et dans le secteur énergétique en général. Nous estimons avoir apporté des réponses et des éléments de réflexions pertinents à l'ensemble des questions de recherche que nous avions formulé en introduction de ce travail. De ce fait, nous sommes globalement satisfaits des résultats obtenus lors de nos analyses. Cependant, nous devons souligner les difficultés rencontrées lors de la phase d'implémentation de notre système « Proof-of-Concept ». Les concepts liés à la mise en place d'une infrastructure « blockchain » nécessitent un panel des compétences spécifiques. En partant d'une implémentation vierge, il est nécessaire d'avoir de bonnes connaissances en développement logiciel et en déploiement d'infrastructures réseau distribuées. Malheureusement, nous n'avons pas été en mesure de démontrer le plein potentiel du système en implémentant les notions « métier » spécifiques au secteur énergétique. De plus, le temps nécessaire à la résolutions des différents problèmes rencontrés à malheureusement été pris au détriment de approfondissement de certaines notions au sein de ce rapport. Nous synthétisons donc notre travail de la manière suivante :

Tableau 23: Synthèse des objectifs atteints et non atteints lors de cette étude

Question de recherche	Synthèse des objectifs atteints et non atteints
RQ1	Nous considérons avoir défini et explorer les concepts fondamentaux liés à la technologie « Blockchain ». Cependant, nous avons survolé certains mécanismes qui auraient pu être approfondis selon nous (ex. : technique de cryptographie et leurs implications dans la définition de l'identité des utilisateurs).
RQ2	Nous sommes parvenus à trouver des exemples d'implémentation particulièrement pertinents dans le cadre de notre thématique. Cependant, nous estimons avoir été trop succincts dans leurs présentations. Un approfondissement des systèmes implémenté et d'éventuels contacts avec les sociétés concernées auraient été pertinents dans le cadre de notre travail.
RQ3	Nous estimons avoir identifié les éléments clés à prendre en considération lors de la sélection d'une plateforme basée sur la « blockchain ». La liste des critères présentés n'est évidemment pas exhaustive, mais elle a le mérite d'adresser les problématiques essentielles.
RQ4	Nous avons brièvement comparé les résultats obtenus par notre système avec l'implémentation de la « blockchain » aux potentiels résultats sans cette dernière. Cependant, nous pensons que cet aspect aurait dû être approfondi dans un chapitre dédié à la comparaison des deux systèmes. Nous n'avons pas réalisé cette analyse supplémentaire due au temps supplémentaire passé sur l'implémentation du système « Proof-of Concept ».

En conclusion de ce rapport, nous souhaitons exprimer le plaisir que nous avons eu durant la réalisation de ce travail, tant sur les aspects théoriques et d'analyses que sur les aspects pratiques liés à l'implémentation. Ce travail nous a permis de découvrir un secteur d'activité riche et complexe, qui devra faire face à de nombreux défis lors des prochaines années. Nous espérons que ce travail contribuera démontrer que bon nombre de ces défis peuvent être solutionnés par une adoption pertinente de la technologie « blockchain ».

6 Références

Advanced Micro Devices, Inc. (2020, février). *Technologie Secure*. https://www.amd.com/fr/technologies/security

Alharby, M., & Moorsel, A. van. (2017). Blockchain Based Smart Contracts : A Systematic Mapping Study. *Computer Science & Information Technology (CS & IT)*, 125-140. https://doi.org/10.5121/csit.2017.71011

Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D., Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector : A systematic review of challenges and opportunities. *Renewable and Sustainable Energy Reviews*, *100*, 143-174. https://doi.org/10.1016/j.rser.2018.10.014

Angelis, S. D., Aniello, L., Baldoni, R., Lombardi, F., Margheri, A., & Sassone, V. (2017). *PBFT vs Proof-of-Authority : Applying the CAP Theorem to Permissioned Blockchain*. 11.

Bach, L. M., Mihaljevic, B., & Zagar, M. (2018). Comparative analysis of blockchain consensus algorithms. *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, 1545-1550. https://doi.org/10.23919/MIPRO.2018.8400278

Bitcoin.com. (2020). *Bitcoin.com—Markets*. Bitcoin.Com | Markets, Price, Charts and News. https://markets.bitcoin.com

Blockchain France Associés. (2016). *La Blockchain décryptée*. Observatoire Netexplo.

Blockchain.com. (2020a, février). *Chart—Blockchain Size*. Blockchain.com. https://www.blockchain.com/charts/blocks-size

Blockchain.com. (2020b, février). *Chart—Median Confirmation Time*. Blockchain.com. https://www.blockchain.com/charts/median-confirmation-time

Boston Consulting Group. (2020, janvier 3). *Automobile : La vente de véhicules électrifiés dépassera celle des véhicules thermiques en 2030*. https://www.bcg.com. https://www.bcg.com/fr-fr/d/press/3jan2020-automobile-la-vente-de-vehicules-electrifies-depassera-celle-des-vehicules-thermiques-en-2030-237045

Buterin, V. (2017, février 6). The Meaning of Decentralization. *Medium*. https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274

Chabert, A. (2018). Getting Started with Hyperledger Fabric. *ChainHero*, 84.

CoinMarketCap. (2020, février). *Top 100 Cryptocurrencies by Market Capitalization*. CoinMarketCap. https://coinmarketcap.com/all/views/all/

ConsenSys Diligence. (2020, janvier). *Known Attacks—Ethereum Smart Contract Best Practices*. https://consensys.github.io/smart-contract-best-practices/known_attacks/

Daniels, A. (2018, octobre 18). The rise of private permissionless blockchains. *Medium*. https://medium.com/ltonetwork/the-rise-of-private-permissionless-blockchains-part-1-4c39bea2e2be

Davidson, M. (2020, janvier 6). *Top 3 enterprise tech trends to watch in 2020*. Computerworld. https://www.computerworld.com/article/3512109/top-3-enterprise-tech-trends-to-watch-in-2020.html

De Quénetain, S. (2018, juin 12). L'arbre de Merkle : La Colonne Vertébrale de la Blockchain. *Blockchains Expert*. https://www.blockchains-expert.com/larbre-de-merkle-colonne-vertebrale-de-blockchain/

Droz, D. (2019, mars 7). *Suisse : Quelle part de voitures électriques?* https://www.arcinfo.ch/dossiers/l-expert-vous-repond/articles/suisse-quelle-part-de-voitures-electriques-824827

Eberhardt, J., & Tai, S. (2017). On or Off the Blockchain? Insights on Off-Chaining Computation and Data. In F. De Paoli, S. Schulte, & E. Broch Johnsen (Éd.), *Service-Oriented and Cloud Computing* (Vol. 10465, p. 3-15). Springer International Publishing. https://doi.org/10.1007/978-3-319-67262-5_1

Encyclopédie Larousse. (2019). *Énergie fossile*. Larousse. https://www.larousse.fr/encyclopedie/divers/énergie_fossile/53118

Energy Web Foundation. (2020, février). *Energy Web*. Energy Web. https://www.energyweb.org/

Ethereum Foundation. (2020, janvier 31). *Ethereum.org*. https://ethereum.org/

Fondation d'entreprise ALCEN pour la Connaissance des énergies. (2019, novembre 8). *Afrique : Un futur énergétique « crucial pour le monde »*. Connaissance des Énergies. https://www.connaissancedesenergies.org/afrique-un-futur-energetique-crucial-pour-le-monde-191108

Foucault-Dumas, C. (2018, juillet 9). *A leur tour, PostFinance et EWB testent la gestion énergétique par la blockchain*. ICT Journal. https://www.ictjournal.ch/news/2018-07-09/a-leur-tour-postfinance-et-ewb-testent-la-gestion-energetique-par-la-blockchain

Galas, G. (2018, mai 15). Analyse et comparaison des mécanismes de consensus dans la blockchain. *Medium*. https://medium.com/@godefroy.galas/analyse-et-comparaison-des-m%C3%A9canismes-de-consensus-dans-la-blockchain-f91aee511ea3

Garg, P. (2020, janvier 27). Bitcoin Gold 51% attack highlights the weaknesses of proof-of-work. *CryptoSlate*. https://cryptoslate.com/bitcoin-gold-51-attack-highlights-the-weaknesses-of-proof-of-work/

Gatteschi, V., Lamberti, F., Demartini, C., Pranteda, C., & Santamaría, V. (2018). To Blockchain or Not to Blockchain : That Is the Question. *IT Professional*, *20*(2), 62-74. https://doi.org/10.1109/MITP.2018.021921652

Global Carbon Project. (2018). *Map view—CO2 Emissions*. http://www.globalcarbonatlas.org/en/CO2-emissions

Grange, E. (2016, février 24). *Mesh World P2P Simulation Hypothesis*. https://www.delphitools.info/DWSH/

Hileman, G., & Rauchs, M. (2017). 2017 Global Blockchain Benchmarking Study. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.3040224

IBM Corporation. (2020, février). *IBM Secure Service Container*. https://www.ibm.com/ch-fr/marketplace/secure-service-container

Intel Corporation. (2020, février). *Intel® Software Guard Extensions*. https://software.intel.com/en-us/sgx

Kuo, T.-T., Zavaleta Rojas, H., & Ohno-Machado, L. (2019). Comparison of blockchain platforms : A systematic review and healthcare examples. *Journal of the American Medical Informatics Association*, *26*(5), 462-478. https://doi.org/10.1093/jamia/ocy185

Lamport, L., Shostak, R., & Pease, M. (1982). The Byzantine Generals Problem. *ACM Transactions on Programming Languages and Systems*, *4*(3), 20.

Litecoin Project. (2020, janvier). *Litecoin—Open source P2P digital currency*. https://litecoin.org/

Maloney, C. (2018, mai 28). *92% of All Blockchain Projects Fail*. Ethereum World News. https://ethereumworldnews.com/92-of-all-blockchain-projects-fail/

Martinez, J. (2018, juin 7). Understanding Proof of Stake : The Nothing at Stake Theory. *Medium*. https://medium.com/coinmonks/understanding-proof-of-stake-the-nothing-at-stake-theory-1f0d71bc027

Mengelkamp, E., Notheisen, B., Beer, C., Dauer, D., & Weinhardt, C. (2018). A blockchain-based smart grid : Towards sustainable local energy markets. *Computer Science - Research and Development*, *33*(1-2), 207-214. https://doi.org/10.1007/s00450-017-0360-9

Microsoft Corporation. (2017, juillet 3). *Configure Distribution in SQL Server*. https://docs.microsoft.com/en-us/sql/relational-databases/replication/configure-distribution

Natoli, C., Yu, J., Gramoli, V., & Esteves-Verissimo, P. (2019). Deconstructing Blockchains : A Comprehensive Survey on Consensus, Membership and Structure. *ArXiv:1908.08316 [Cs]*. http://arxiv.org/abs/1908.08316

Nebulous, Inc. (2020, février). *Sia—Decentralized storage for the post-cloud world*. https://sia.tech/

NeonVest. (2019, janvier 15). The Scalability Trilemma in Blockchain. *Medium*. https://medium.com/@aakash_13214/the-scalability-trilemma-in-blockchain-75fb57f646df

Odisi, F. (2020, janvier 31). Intro to Challenges of Upgrading Smart Contracts in Ethereum with Solidity. *Medium*. https://levelup.gitconnected.com/introduction-to-ethereum-smart-contract-upgradability-with-solidity-789cc497c56f

Oracle Corporation. (2002). *Oracle—Distributed Database Concepts*. https://docs.oracle.com/cd/B10501_01/server.920/a96521/ds_concepts.htm

Panetta, K. (2018). *5 Trends Emerge in the Gartner Hype Cycle for Emerging Technologies, 2018*. Gartner, Inc. //www.gartner.com/smarterwithgartner/5-trends-emerge-in-gartner-hype-cycle-for-emerging-technologies-2018/

Panetta, K. (2019a). *5 Trends Appear on the Gartner Hype Cycle for Emerging Technologies, 2019*. Gartner, Inc. // www.gartner.com/smarterwithgartner/5-trends-appear-on-the-gartner-hype-cycle-for-emerging-technologies-2019/

Panetta, K. (2019b). *Gartner Top 10 Strategic Technology Trends for 2020*. Gartner, Inc. //www.gartner.com/smarterwithgartner/gartner-top-10-strategic-technology-trends-for-2020/

Parlement européen. (2018, janvier 10). *Clean energy : The EU's push for renewables and energy efficiency*. https://www.europarl.europa.eu/news/en/headlines/economy/20180109STO91387/mitigating-climate-change-with-the-eu-s-clean-energy-policy

Pezet, J. (2017, octobre 13). *Que signifie «disruptif» et pourquoi tout le monde sort ce mot ?* Libération.fr. https://www.liberation.fr/desintox/2017/10/13/que-signifie-disruptif-et-pourquoi-tout-le-monde-sort-ce-mot_1602934

Pignon, V. (2017). *L'Etat de Genève expérimente la technologie Blockchain*. République et canton de Genève. https://www.ge.ch/blog/geneve-lab/etat-geneve-experimente-technologie-blockchain-6-10-2017

Plain, N. (2019, janvier 7). *Blockchain et accès à l'électricité renouvelable dans le monde*. https://www.youtube.com/watch?v=9p64BdTe78k

Pleynet, J.-B. (2017, juin 11). Le chiffrage à clés publiques / privées expliqué aux non initiés. *Medium*. https://medium.com/@JB_Pleynet/le-chiffrage-%C3%A0-cl%C3%A9s-publiques-priv%C3%A9s-expliqu%C3%A9-aux-non-initi%C3%A9s-1a0eed15934f

PostgreSQL wiki. (2018, septembre 12). *Replication, Clustering, and Connection Pooling*. https://wiki.postgresql.org/wiki/Replication,_Clustering,_and_Connection_Pooling

Protocol Labs. (2020, février). *IPFS Powers the Distributed Web*. IPFS. https://ipfs.io/

PwC. (2016). *Blockchain – an opportunity for energy producers and consumers ?* PricewaterhouseCoopers.

Queijo, A. (2017, décembre 1). *Les services industriels de six villes suisses coopèrent dans la blockchain*. ICT Journal. https://www.ictjournal.ch/news/2017-12-01/les-services-industriels-de-six-villes-suisses-cooperent-dans-la-blockchain

Rimol, M. (2019). *Gartner 2019 Hype Cycle for Blockchain Business Shows Blockchain Will Have a Transformational Impact across Industries in Five to 10 Years*. Gartner, Inc. https://www.gartner.com/en/newsroom/press-releases/2019-09-12-gartner-2019-hype-cycle-for-blockchain-business-shows

Ripple, Inc. (2020, janvier). *XRP - A Digital Asset Built for Global Payments*. Ripple. https://ripple.com/xrp/

SCCER-FURIES. (2020a, février). *Context – SCCER-FURIES*. https://www.epfl.ch/research/domains/sccer-furies/whoweare/context/

SCCER-FURIES. (2020b, février). *Who We Are – SCCER-FURIES*. https://www.epfl.ch/research/domains/sccer-furies/whoweare/

Schweiz, E. (2020, février). *Energies renouvelables*. SuisseEnergie. https://www.suisseenergie.ch/page/fr-ch/energies-renouvelables

SFOE, S. F. O. of E. (2018, janvier 18). *Energy Strategy 2050*. https://www.bfe.admin.ch/bfe/en/home/politik/energiestrategie-2050.html

Sharma, T. K. (2019a, mai 11). Top 10 Blockchain Platforms You Need To Know About. *Blockchain Council*. https://www.blockchain-council.org/blockchain/top-10-blockchain-platforms-you-need-to-know-about/

Sharma, T. K. (2019b, juillet 3). Top 10 Promising Blockchain Use Cases. *Blockchain Council*. https://www.blockchain-council.org/blockchain/top-10-promising-blockchain-use-cases/

Soudoplatoff, S., & Caseau, Y. (2016). La blockchain ou la confiance distribuée. *Fondation pour l'innovation politique*, 52.

Swarm. (2020, février). *Swarm—Storage and Communication for a Sovereign Digital Society*. https://www.ethereum.org/swarm

The Linux Foundation. (2019a). *Ledger—Hyperledger*. https://hyperledger-fabric.readthedocs.io/en/release-1.4/ledger/ledger.html

The Linux Foundation. (2019b). *Peers—Hyperledger*. https://hyperledger-fabric.readthedocs.io/en/release-1.4/peers/peers.html

Vianin, J. (2018). *EV Blockchain Charging : Système de facturation autonome pour recharge des voitures électriques basé sur la blockchain*. HES-SO.

Viriyasitavat, W., & Hoonsopon, D. (2019). Blockchain characteristics and consensus in modern business processes. *Journal of Industrial Information Integration*, *13*, 32-39. https://doi.org/10.1016/j.jii.2018.07.004

Wagner, S. (2019, juin 19). *Energie Wasser Berne teste la recharge de véhicules électriques par la blockchain*. ICT Journal. https://www.ictjournal.ch/news/2019-06-19/energie-wasser-berne-teste-la-recharge-de-vehicules-electriques-par-la-blockchain

Wessbecher, L. (2018, mai 17). Ce que la blockchain peut apporter à l'industrie du film. *France 24*. https://www.france24.com/fr/20180517-blockchain-peut-apporter-a-industrie-film

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*, 557-564. https://doi.org/10.1109/BigDataCongress.2017.85

Zhou, K., Taigang Liu, & Lifeng Zhou. (2015). Industry 4.0 : Towards future industrial opportunities and challenges. *2015 12th International Conference on Fuzzy Systems and Knowledge Discovery (FSKD)*, 2147-2152. https://doi.org/10.1109/FSKD.2015.7382284

7 Annexes

7.1 Hyperledger Global Forum 2018 – Workshop

Getting Started with Hyperledger Fabric

Using Golang

Antoine Chabert, Research & Development Leader at ChainHero,
Hyperledger, *The Linux Foundation*

The objective

How to start writing a full-stack Golang application that interact with a blockchain: Hyperledger Fabric?

What will NOT be covered in the session ?

- How Hyperledger Fabric works in deep → hyperledger-fabric.readthedocs.io/en/latest/
- How generate and configure an Hyperledger Fabric Network→ github.com/chainHero/heroes-service-network hyperledger-fabric.readthedocs.io/en/latest/build_network.html
- How to configure the Fabric SDK Go→ github.com/hyperledger/fabric-sdk-go/blob/master/test/fixtures/config/config_e2e.yaml
- Get best practices for a production use
- How to write in Golang
- …

Who are we?

CHAINHERO

chainHero, is dedicated to help companies and governments to build and deploy public or permissioned blockchains.

Our references…

Notaires de France

VINCI

AXA

Civis Blockchain

sada assurances Groupe DEVK

HYPERLEDGER
amazon web services
IBM Bluemix
ethereum
CHAINHERO
circleci
golang
docker
ANGULAR
React
node

Montpellier Méditerranée Métropole

IBM

LIRMM

AXenS
Transforming Global Trade

Who am I?

An engineer from the *Institut National des Sciences Appliquées* (INSA) Lyon, France.

Attended *École Polytechnique Fédéral de Lausanne* (EPFL), Switzerland.

Web experiences at Smile Open Source and Worldline, ATOS.

Head of R&D department at Chainhero for last 2 years.

1. How to start ?
2. What are we going to build ?
3. Reminder: Hyperledger Fabric
4. How to launch your first network ?
5. How to write your first chaincode ?
6. How to build your first application ?
7. Exercises

1

The environment for exercises

Linux is required, with:

- Docker
- Docker-compose
- Golang
- Dep (Go dependency management tool)
- Make

You can use this prepared virtual machine (using VirtualBox) to follow this session on your computer (user: `hlgf` / password: `fabric`):

https://chainhero.io/hlgf-ws-vm

2. What are we going to build?

CHAINHERO

2

The application

Build a collaborative resource management system.

2

Blockchain, why ?

The management of resources via the blockchain can allow a better traceability while simplifying the procedures.

The resource could be anything. For example, a vehicle that is used in a corporation. This way it is possible to identify who has used it over time or to automate vehicle availability.

2

The data structure

Admin

Person who proposes and manages resources for consumers.

Attributes

- *Name*

Consumer

A person who can acquire and then release a resource.

Attributes

- *Name*

Resource

Object, tool, good, service... which is manageable and consumable.

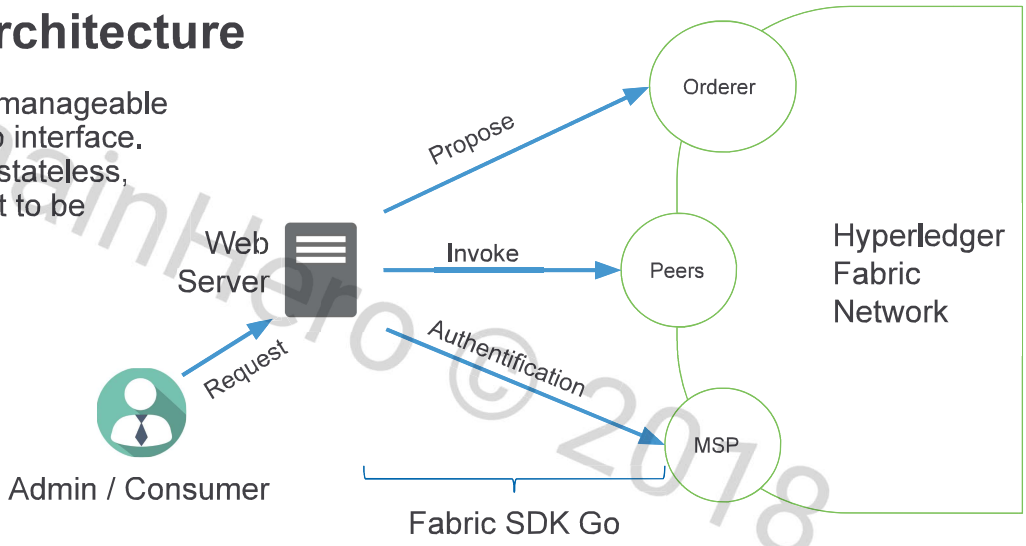
Attributes

- *Identifier*
- *Description*
- *Available*
- *Mission*
- *Consumer*

2

The architecture

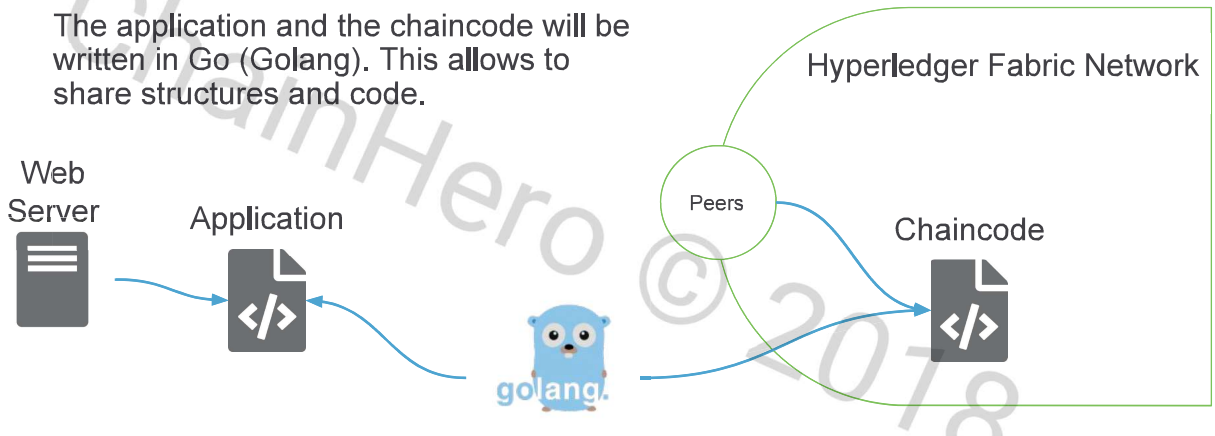
Everything is manageable through a web interface. The server is stateless, which allows it to be decentralized.



2

The architecture

The application and the chaincode will be written in Go (Golang). This allows to share structures and code.

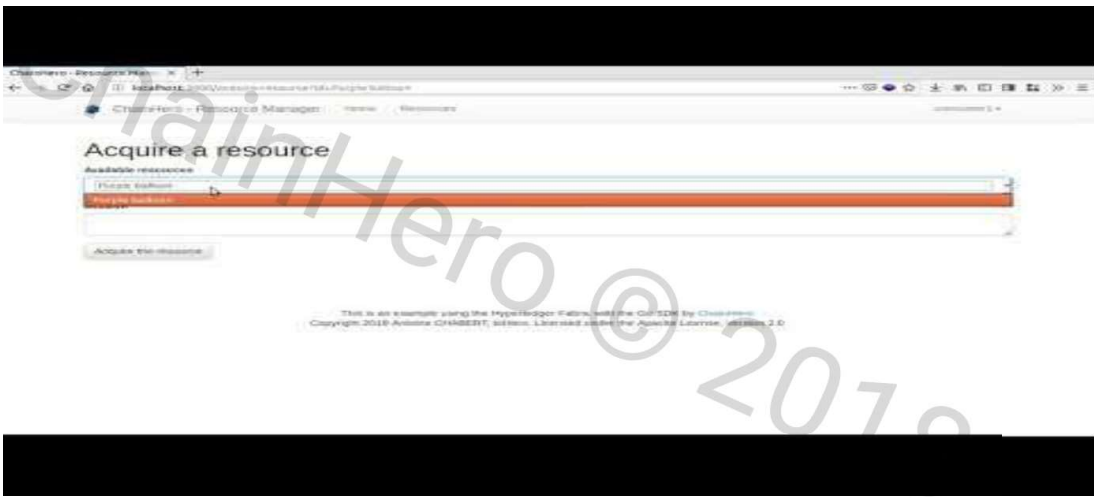


2

Admin

2

Consumer



2

Scenario

CREATE A RESOURCE

Step 1

An **admin** creates a resource and makes it available to **consumers**.

ACQUIRE A RESOURCE

Step 2

A **consumer** acquires an available resource and informs for which mission.

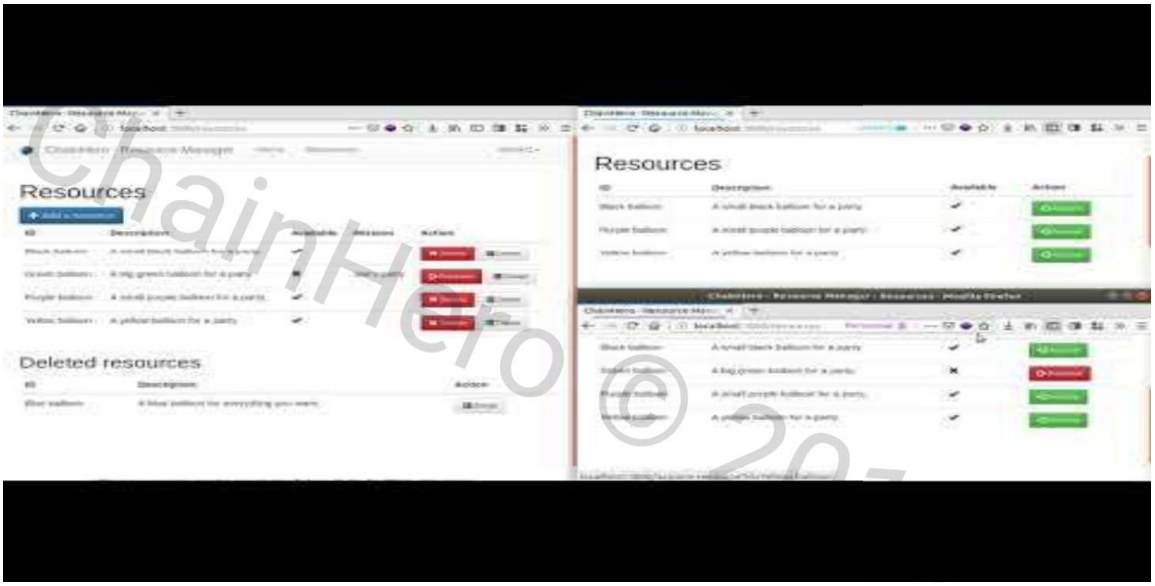
RELEASE A RESOURCE

Step 3

A **consumer** releases a resource, which then becomes available.

2

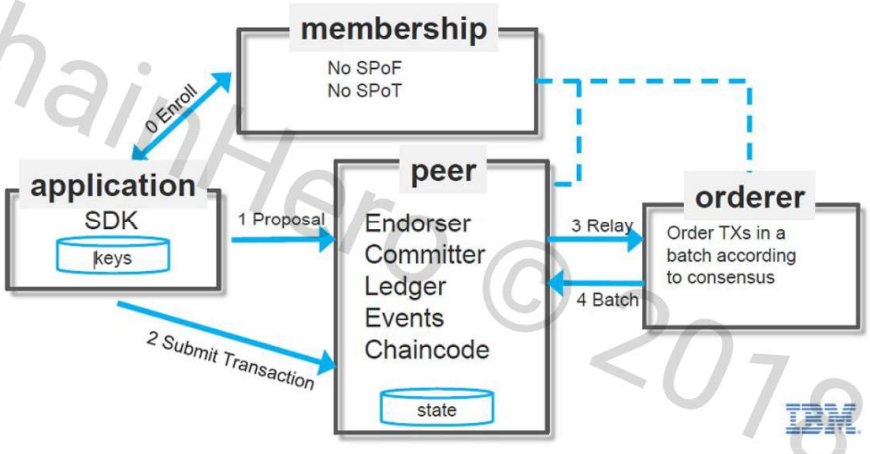
Scenario



3. Reminder: Hyperledger Fabric

3

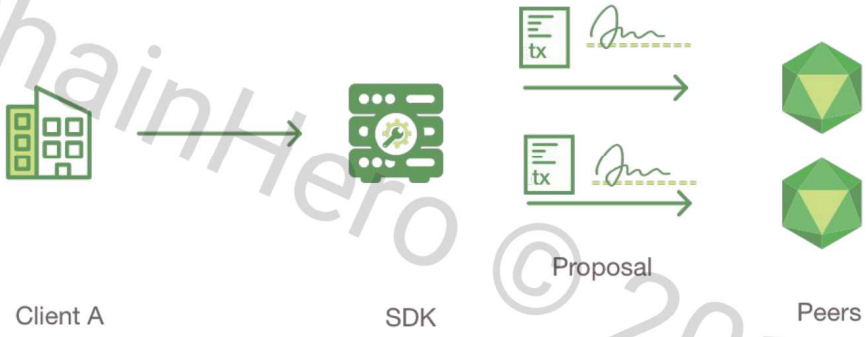
Hyperledger Fabric: architecture



3

Hyperledger Fabric: transaction flow 1

initialization

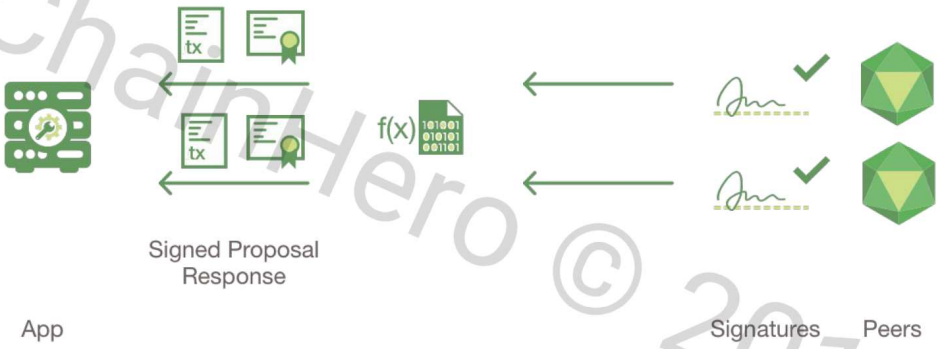


Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction flow 2

Endorsement

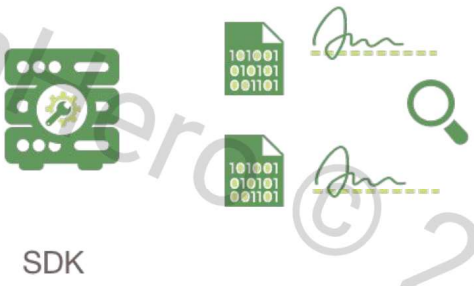


Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction flow 3

Verification



Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction flow 4

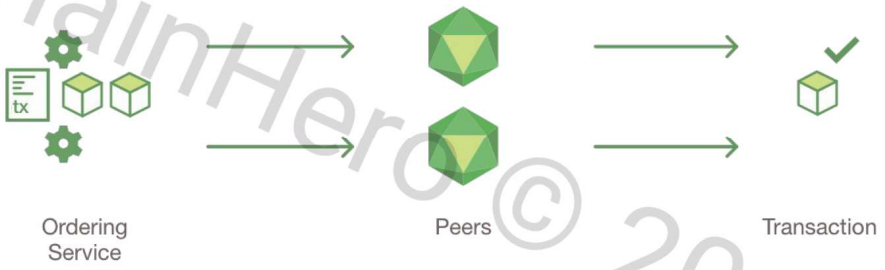
Ordering transaction

Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction flow 5

Validation & Commitment

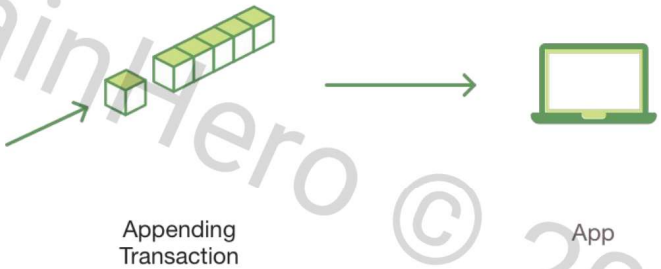


Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction flow 6

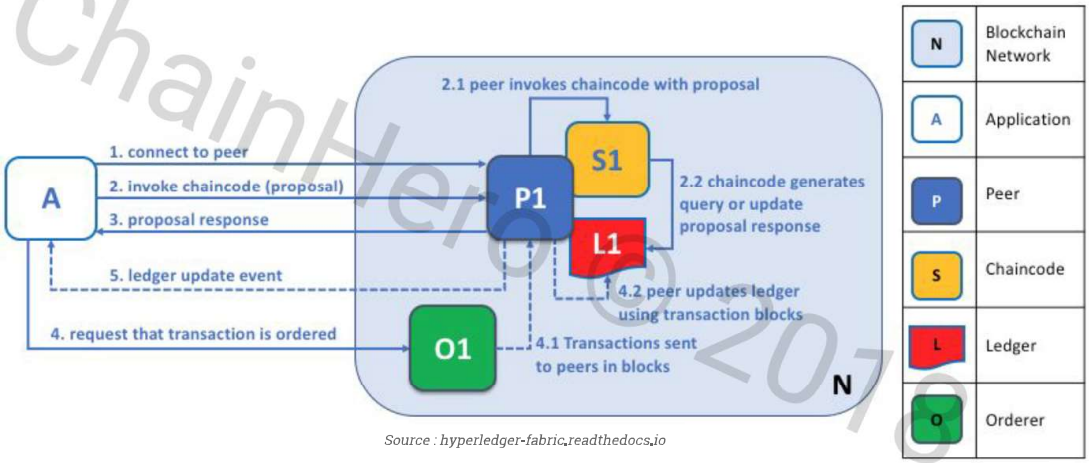
Update ledger



Source : hyperledger-fabric.readthedocs.io

3

Hyperledger Fabric: transaction summary



Source : hyperledger-fabric.readthedocs.io

4. How to launch your first network ?

4

How many components ?

PROPOSAL

MSP :
- 1x admins and consumers consortium

Peers :
- Minimum 1x admin
- Minimum 1x consumer

Orderers :
- Minimum 4 (in cluster mode)

Channel :
- 1x for resources, admins, consumers

4

How many components in development ?

MSP :
- 1x admins and consumers consortium

Peers :
- 1x or 2x

Orderers :
- 1x (in solo mode)

Channel :
- 1x for resources, admins, consumers

4

Get ready to start...

- Create folders :

```
~/go/src/github.com/chainHero/resource-manager
```

- Go into it (`cd ~/go/src/...`)
- Checkout the starter kit :

```
git clone https://github.com/chainHero/resource-manager.git ./
```

- Checkout the first step branch :

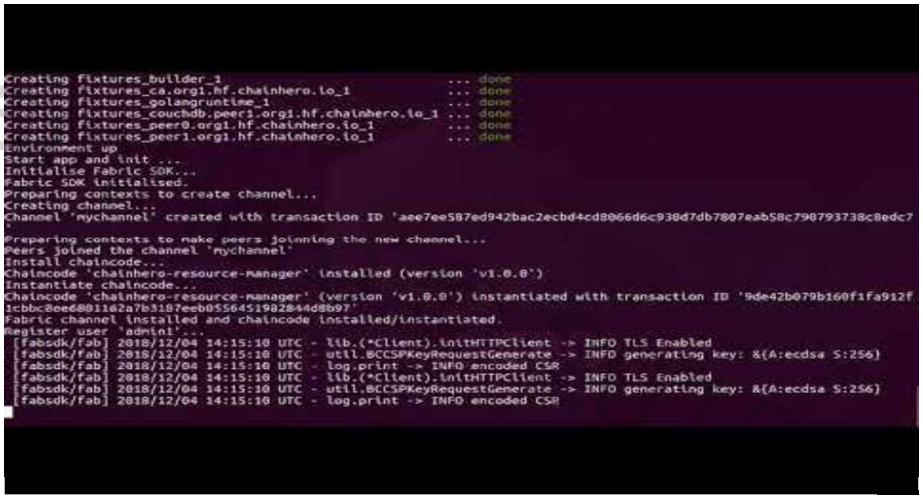
```
git checkout step_1
```


4

Start the development network !

Run :

```
make
```



4

What's going on behind the scene?

- Some clean up if you previously start the application
- Launch the network using `docker-compose`
- Initialise the application in order to :
  - Prepare Fabric SDK to communicate with the network
  - Create the channel (named "`mychannel`")
  - Install and then instantiate the chaincode provided
- Register 3 users (name / password):
  - `admin1 / password`
  - `consumer1 / password`
  - `consumer2 / password`
- Start the web server

4

Going further

```
hlgf:~/go/src/github.com/chainHero/resource-manager$ ll
total 32
drwxr-xr-x 5 ancha ancha  4096 déc.   4 15:28 app/
drwxr-xr-x 4 ancha ancha  4096 déc.   4 15:28 chaincode/
drwxr-xr-x 5 ancha ancha  4096 déc.   3 10:05 fixtures/
-rw-r--r-- 1 ancha ancha 10261 déc.   3 09:41 LICENSE
-rw-r--r-- 1 ancha ancha  1770 déc.   4 10:01 Makefile
-rw-r--r-- 1 ancha ancha   485 déc.   3 17:59 README.md
```


4

Inside `fixtures`

```
hlgf:~/go/src/github.com/chainHero/resource-manager/fixtures$ ll -a
total 32
drwxr-xr-x 5 ancha ancha 4096 déc.   3 10:05 ./
drwxr-xr-x 8 ancha ancha 4096 déc.   4 10:23 ../
drwxr-xr-x 3 ancha ancha 4096 déc.   3 09:41 artifacts/
drwxr-xr-x 4 ancha ancha 4096 déc.   3 09:31 crypto-config/
-rw-r--r-- 1 ancha ancha 6459 déc.   3 10:03 docker-compose.yaml
drwxr-xr-x 2 ancha ancha 4096 déc.   3 10:05 env/
-rw-r--r-- 1 ancha ancha 2390 déc.   3 10:05 .env
```

4

Inside `fixtures` > `artifacts`

```
hlgf:~/go/src/github.com/chainHero/resource-manager/fixtures/artifacts$ ll
total 12
-rw-r--r-- 1 ancha ancha 6561 déc.   3 09:41 genesis.block
drwxr-xr-x 2 ancha ancha 4096 déc.   3 09:41 mychannel/
hlgf:~/go/src/github.com/chainHero/resource-manager/fixtures/artifacts$ ll mychannel/
total 8
-rw-r--r-- 1 ancha ancha 1303 déc.   3 09:41 channel.tx
-rw-r--r-- 1 ancha ancha  289 déc.   3 09:41 org1.anchors.tx
```


4

How to get `crypto-config` and `artifacts` ?

Fabric provide binaries to generate the genesis block for orderers and the channel.

For development, Fabric provided also a binary that generate all certificates for all components and users.

4

How do we know if everything is okay?

Check that every docker containers are up and running with :

```
docker-compose ps
docker ps -a
```

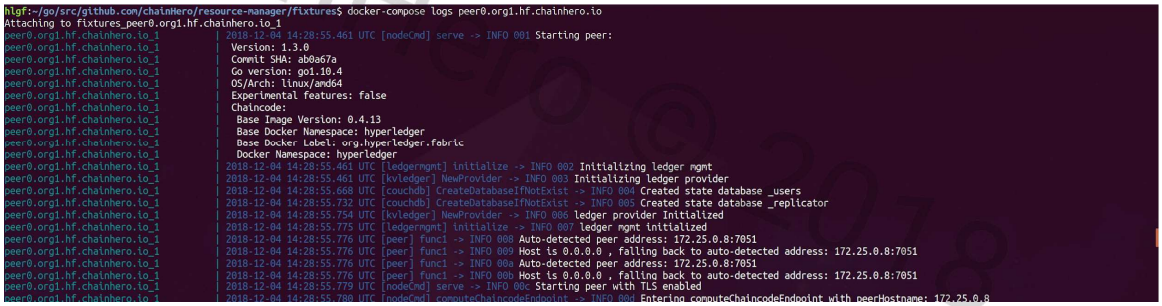
```
hlgf:~/go/src/github.com/chainHero/resource-manager/fixtures$ docker-compose ps
                Name                              Command               State                    Ports
-------------------------------------------------------------------------------------------------------------------------
fixtures_builder_1                          tail -F anything                 Up
fixtures_ca.org1.hf.chainhero.io_1          sh -c fabric-ca-server sta ...   Up      0.0.0.0:7054->7054/tcp
fixtures_couchdb.peer0.org1.hf.chainhero.io_1   tini -- /docker-entrypoint ...   Up      4369/tcp, 0.0.0.0:5984->5984/tcp, 9100/tcp
fixtures_couchdb.peer1.org1.hf.chainhero.io_1   tini -- /docker-entrypoint ...   Up      4369/tcp, 0.0.0.0:6984->5984/tcp, 9100/tcp
fixtures_golangruntime_1                    tail -F anything                 Up
fixtures_orderer.hf.chainhero.io_1          orderer                          Up      0.0.0.0:7050->7050/tcp
fixtures_peer0.org1.hf.chainhero.io_1       peer node start                  Up      0.0.0.0:7051->7051/tcp, 7052/tcp
fixtures_peer1.org1.hf.chainhero.io_1       peer node start                  Up      0.0.0.0:7061->7051/tcp, 7052/tcp
```

4

How do we know if everything is okay?

Check logs of docker containers with :

```
docker-compose logs <container>
docker logs <container>
```



5. How to write your first chaincode ?

5

The interface of a chaincode

```
type Chaincode interface {
  // Init is called during Instantiate transaction after the chaincode container
  // has been established for the first time, allowing the chaincode to
  // initialize its internal data
  Init(stub ChaincodeStubInterface) pb.Response

  // Invoke is called to update or query the ledger in a proposal transaction.
  // Updated state variables are not committed to the ledger until the
  // transaction is committed.
  Invoke(stub ChaincodeStubInterface) pb.Response
}
```


Source : godoc.org/github.com/hyperledger/fabric/core/chaincode/shim#Chaincode

5

How to manage the ledger ?

```
type ChaincodeStubInterface interface {
  GetFunctionAndParameters() (string, []string)
  GetTxID() string
  GetState(key string) ([]byte, error)
  PutState(key string, value []byte) error
  DelState(key string) error
  GetQueryResult(query string) (StateQueryIteratorInterface, error)
  GetHistoryForKey(key string) (HistoryQueryIteratorInterface, error)
  GetCreator() ([]byte, error)
  GetTxTimestamp() (*timestamp.Timestamp, error)
  // [...]
}
```

Source : godoc.org/github.com/hyperledger/fabric/core/chaincode/shim#ChaincodeStubInterface

5

How to check the identity of the user ?

Using the provided package CID

```
type ClientIdentity interface {
  GetID() (string, error)
  GetMSPID() (string, error)
  GetAttributeValue(attrName string) (value string, found bool, err error)
  AssertAttributeValue(attrName, attrValue string) error
  GetX509Certificate() (*x509.Certificate, error)
}
```

Source : godoc.org/github.com/hyperledger/fabric/core/chaincode/lib/cid#ClientIdentity

5

What is provided in the "`step 1`" branch?

```
hlgf:~/go/src/github.com/chainHero/resource-manager/chaincode$ ll
total 52
-rw-r--r-- 1 ancha ancha 12964 déc.   4 15:28 Gopkg.lock
-rw-r--r-- 1 ancha ancha   713 déc.   3 10:07 Gopkg.toml
-rw-r--r-- 1 ancha ancha  2840 déc.   5 10:13 main.go
drwxr-xr-x 2 ancha ancha  4096 déc.   5 10:13 model/
-rw-r--r-- 1 ancha ancha  7646 déc.   5 10:13 query.go
-rw-r--r-- 1 ancha ancha  4143 déc.   5 10:13 update.go
-rw-r--r-- 1 ancha ancha  2964 déc.   3 10:27 util.go
drwxr-xr-x 7 ancha ancha  4096 déc.   4 15:28 vendor/
```

5

Making your life easier... `util.go`

```
func getFromLedger(stub ChaincodeStubInterface, objectType string, id string, result
interface{}) error {
  // [...]
}
func updateInLedger(stub ChaincodeStubInterface, objectType string, id string,
object interface{}) error {
  // [...]
}
func deleteFromLedger(stub ChaincodeStubInterface, objectType string, id string)
error {
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/util.go

5

No magic !

```
func getFromLedger(stub CSI, objectType string, id string, result interface{}) error {
  // [...]
  resultAsByte, err = stub.GetState(key)
  if err != nil {
     return fmt.Errorf("unable to retrieve the object in the ledger: %v", err)
  }
  // [...]
  return nil
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/util.go

5

What is provided in the "`step 1`" branch?

```
hlgf:~/go/src/github.com/chainHero/resource-manager/chaincode$ ll
total 52
-rw-r--r-- 1 ancha ancha 12964 déc.   4 15:28 Gopkg.lock
-rw-r--r-- 1 ancha ancha   713 déc.   3 10:07 Gopkg.toml
-rw-r--r-- 1 ancha ancha  2840 déc.   5 10:13 main.go
drwxr-xr-x 2 ancha ancha  4096 déc.   5 10:13 model/
-rw-r--r-- 1 ancha ancha  7646 déc.   5 10:13 query.go
-rw-r--r-- 1 ancha ancha  4143 déc.   5 10:13 update.go
-rw-r--r-- 1 ancha ancha  2964 déc.   3 10:27 util.go
drwxr-xr-x 7 ancha ancha  4096 déc.   4 15:28 vendor/
```

5

Why a package `model` ?

The "`model`" package contains all the structures and constants that can be useful for both the chaincode and the application.

Putting it in a separate package allows you to import it into the application.

5

Why a package `model` ?

```go
// [...]
type Resource struct {
  ID          string `json:"id"`
  Description string `json:"description"`
  Available   bool   `json:"available"`
  Mission     string `json:"mission,omitempty"`
  Consumer    string `json:"consumer,omitempty"`
}
// [...]
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/model/model.go

5

What is provided in the "`step 1`" branch?

```
hlgf:~/go/src/github.com/chainHero/resource-manager/chaincode$ ll
total 52
-rw-r--r-- 1 ancha ancha 12964 déc.   4 15:28 Gopkg.lock
-rw-r--r-- 1 ancha ancha   713 déc.   3 10:07 Gopkg.toml
-rw-r--r-- 1 ancha ancha  2840 déc.   5 10:13 main.go
drwxr-xr-x 2 ancha ancha  4096 déc.   5 10:13 model/
-rw-r--r-- 1 ancha ancha  7646 déc.   5 10:13 query.go
-rw-r--r-- 1 ancha ancha  4143 déc.   5 10:13 update.go
-rw-r--r-- 1 ancha ancha  2964 déc.   3 10:27 util.go
drwxr-xr-x 7 ancha ancha  4096 déc.   4 15:28 vendor/
```

5

How to manage different kinds of invocation?

```
func (t *ResourceManagerChaincode) Invoke(stub shim.ChaincodeStubInterface) pb.Response {
  function, args := stub.GetFunctionAndParameters()
  if function != "invoke" {
    return shim.Error("Unknown function call")
  }
  if len(args) < 1 {
    return shim.Error("The number of arguments is insufficient.")
  }
  if args[0] == "query" {
    return t.query(stub, args[1:])
  }
  if args[0] == "update" {
    return t.update(stub, args[1:])
  }
  return shim.Error("Unknown action, check the first argument")
}
```

Go to `query.go` file

Go to `update.go` file

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/main.go

5

Why split read and write requests?

The manipulations to be done on the application side are different.

In the case of a reading, you only need to go to the "`endorsement`" phase.

For writing, it is necessary to submit a transaction and therefore go through "`ordering`" phase.

5

Query `admin` : explanations 1

```
func (t *ResourceManagerChaincode) query(stub CSI, args []string) pb.Response {
  if len(args) < 1 {
    return shim.Error("The number of arguments is insufficient.")
  }
  // [...]
  if args[0] == "admin" {
    return t.admin(stub, args[1:])
  }
  // [...]
  return shim.Error("Unknown query action, check the second argument.")
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/query.go

5

Query `admin` : explanations 2

```
func (t *ResourceManagerChaincode) admin(stub CSI, args []string) pb.Response {
  err := cid.AssertAttributeValue(stub, model.ActorAttribute, model.ActorAdmin)
  if err != nil {
    return shim.Error(fmt.Sprintf("Only admin is allowed for the kind of request: %v", err))
  }
  adminID, err := cid.GetID(stub)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable to identify the ID of the request owner: %v", err))
  }
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/query.go

5

Query `admin` : explanations 3

```
func (t *ResourceManagerChaincode) admin(stub CSI, args []string) pb.Response {
  // [...]
  var admin model.Admin
  err = getFromLedger(stub, model.ObjectTypeAdmin, adminID, &admin)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable to retrieve admin in the ledger: %v", err))
  }
  adminAsByte, err := objectToByte(admin)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable convert the admin to byte: %v", err))
  }
  return shim.Success(adminAsByte)
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/query.go

5

Update `register` : explanations 1

```
func (t *ResourceManagerChaincode) update(stub CSI, args []string) pb.Response {
  if len(args) < 1 {
    return shim.Error("The number of arguments is insufficient.")
  }
  if args[0] == "register" {
    return t.register(stub, args[1:])
  }
  // [...]
  return shim.Error("Unknown update action, check the second argument.")
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/update.go

5 Update `register` : explanations 2

```
func (t *ResourceManagerChaincode) register(stub CSI, args []string) pb.Response {
  actorType, found, err := cid.GetAttributeValue(stub, model.ActorAttribute)
  if err != nil {
     return shim.Error(fmt.Sprintf("Unable to identify the the request owner: %v", err))
  }
  if !found {
     return shim.Error("The type of the request owner is not present")
  }
  if len(args) < 1 {
     return shim.Error("The number of arguments is insufficient.")
  }
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/update.go

5 Update `register` : explanations 3

```
func (t *ResourceManagerChaincode) register(stub CSI, args []string) pb.Response {
  // [...]
  actorID, err := cid.GetID(stub)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable to identify the ID of the owner: %v", err))
  }
  switch actorType {
  case model.ActorAdmin:
    // [...]
  case model.ActorConsumer:
    // [...]
  }
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/update.go

5 Update `register` : explanations 4

```
func (t *ResourceManagerChaincode) register(stub CSI, args []string) pb.Response {
  // [...]
  case model.ActorAdmin:
    newAdmin := model.Admin{Actor: model.Actor{ID: actorID, Name: args[0]}}
    err = updateInLedger(stub, model.ObjectTypeAdmin, actorID, newAdmin)
    if err != nil {
       return shim.Error(fmt.Sprintf("Unable to update in the ledger: %v", err))
    }
    // [...]
  }
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/chaincode/update.go

5

How can I test my chaincode?

Fabric provides a mock interface to perform unit tests on your chaincode. However, this remains very limited, no identity management or consistency in transactions.

The best way, deploy the chaincode and perform call testing via an SDK or CLI.

6. How to build your first application ?

6

What is provided in the "`step 1`" branch?

```
hlgf:~/go/src/github.com/chainHero/resource-manager/app$ ll
total 60
-rw-r--r-- 1 ancha ancha 17548 déc.   3 10:07 config.yaml
drwxr-xr-x 2 ancha ancha  4096 déc.   5 11:07 fabric/
-rw-r--r-- 1 ancha ancha 17088 déc.   4 15:28 Gopkg.lock
-rw-r--r-- 1 ancha ancha   784 déc.   3 10:07 Gopkg.toml
-rw-r--r-- 1 ancha ancha  3256 déc.   3 10:07 main.go
drwxr-xr-x 6 ancha ancha  4096 déc.   4 15:28 vendor/
drwxr-xr-x 5 ancha ancha  4096 déc.   5 11:07 web/
```

6

What happens in the "main.go" file?

- Retrieve some flags from the CLI
- Prepare and initialise the Fabric SDK
- Create channel and install/instantiate chaincode is asked in CLI
- Register users if asked in CLI
- Run the web server

6

Where are the requests to the chaincode?

```
hlgf:~/go/src/github.com/chainHero/resource-manager/app$ ll
total 60
-rw-r--r-- 1 ancha ancha 17548 déc.   3 10:07 config.yaml
drwxr-xr-x 2 ancha ancha  4096 déc.   5 11:07 fabric/
-rw-r--r-- 1 ancha ancha 17088 déc.   4 15:28 Gopkg.lock
-rw-r--r-- 1 ancha ancha   784 déc.   3 10:07 Gopkg.toml
-rw-r--r-- 1 ancha ancha  3256 déc.   3 10:07 main.go
drwxr-xr-x 6 ancha ancha  4096 déc.   4 15:28 vendor/
drwxr-xr-x 5 ancha ancha  4096 déc.   5 11:07 web/
hlgf:~/go/src/github.com/chainHero/resource-manager/app$ ll fabric/
total 20
-rw-r--r-- 1 ancha ancha 3052 déc.   5 11:07 query.go
-rw-r--r-- 1 ancha ancha 8717 déc.   4 10:02 setup.go
-rw-r--r-- 1 ancha ancha 2017 déc.   5 11:07 update.go
```


6

What does a query look like?

```go
func (u *User) query(args [][]byte, responseObject interface{}) error {
  response, err := u.ChannelClient.Query(
    channel.Request{
      ChaincodeID: u.Fabric.ChaincodeID,
      Fcn: "invoke",
      Args: append([][]byte{[]byte("query")}, args...),
    },
    channel.WithRetry(retry.DefaultChannelOpts),
  )
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/query.go

6

What does a query look like?

```
func (u *User) query(args [][]byte, responseObject interface{}) error {
  // [...]
  if responseObject != nil {
    err = json.Unmarshal(response.Payload, responseObject)
    if err != nil {
      return fmt.Errorf("unable to convert response to the object given: %v", err)
    }
  }
  return nil
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/query.go

6

And so the `admin` query?

```
func (u *User) QueryAdmin() (*model.Admin, error) {
  var admin *model.Admin
  err := u.query([][]byte{[]byte("admin")}, &admin)
  if err != nil {
    return nil, err
  }
  return admin, nil
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/query.go

6

What does an update look like?

```
func (u *User) update(args [][]byte, responseObject interface{}) error {
  response, err := u.ChannelClient.Execute(
    channel.Request{
      ChaincodeID: u.Fabric.ChaincodeID,
      Fcn: "invoke",
      Args: append([][]byte{[]byte("update")}, args...),
    },
    channel.WithRetry(retry.DefaultChannelOpts),
  )
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/update.go

6

What does an update look like?

```
func (u *User) update(args [][]byte, responseObject interface{}) error {
  // [...]
  if responseObject != nil {
    err = json.Unmarshal(response.Payload, responseObject)
    if err != nil {
      return fmt.Errorf("unable to convert response to the object given: %v", err)
    }
  }
  return nil
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/update.go

6

And so the `register` update?

```
func (u *User) UpdateRegister() error {
  return u.update([][]byte{[]byte("register"), []byte(u.Username)}, nil)
}
```

Source : github.com/chainHero/resource-manager/blob/step_1/app/fabric/update.go

7. Exercises

7

Solve the `step 1`

There are blanks in the code of the first step, in particular it is not possible to add resources for an admin user.

You must replace the TODO in these two files:

- github.com/chainHero/resource-manager/blob/step_1/app/fabric/update.go#L53
- github.com/chainHero/resource-manager/blob/step_1/chaincode/update.go#L116

7

Solutions for the `step 1`

Checkout the branch "`step_1_solved`" or look at there :

- github.com/chainHero/resource-manager/blob/step_1_solved/app/fabric/update.go
- github.com/chainHero/resource-manager/blob/step_1_solved/chaincode/update.go

7

Solutions for the `step 1`

```
func (u *User) UpdateAdd(resourceID, resourceDescription string) error {
  return u.update(
    [][]byte{[]byte("add"), []byte(resourceID), []byte(resourceDescription)},
    nil,
  )
}
```

Source : github.com/chainHero/resource-manager/blob/step_1_solved/app/fabric/update.go#L52

7 Solutions for the step 1

```go
func (t *ResourceManagerChaincode) add(stub CSI, args []string) pb.Response {
  fmt.Println("# add resource")
  err := cid.AssertAttributeValue(stub, model.ActorAttribute, model.ActorAdmin)
  if err != nil {
    return shim.Error(fmt.Sprintf("Only admin is allowed for this request: %v", err))
  }
  // [...]
}
```

Source : github.com/chainHero/resource-manager/blob/step_1_solved/chaincode/update.go#L114

7 Solutions for the step 1

```go
func (t *ResourceManagerChaincode) add(stub CSI, args []string) pb.Response {
  // [...]
  if len(args) < 2 {
    return shim.Error("The number of arguments is insufficient.")
  }
  resourceID := args[0]
  if resourceID == "" {
    return shim.Error("The resource ID is empty.")
  }
  resourceDescription := args[1]
  if resourceDescription == "" {
    return shim.Error("The resource description is empty.")
  }
  // [...]
}
```


7 Solutions for the step 1

```go
func (t *ResourceManagerChaincode) add(stub CSI, args []string) pb.Response {
  // [...]
  resource := model.Resource{
    ID:          resourceID,
    Description: resourceDescription,
    Available:   true,
  }
  err = updateInLedger(stub, model.ObjectTypeResource, resourceID, resource)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable to create the resource in the ledger: %v", err))
  }
  // [...]
}
```

7

Solutions for the step 1

```
func (t *ResourceManagerChaincode) add(stub CSI, args []string) pb.Response {
  // [...]
  resourceAsByte, err := objectToByte(resource)
  if err != nil {
    return shim.Error(fmt.Sprintf("Unable convert the resource to byte: %v", err))
  }
  return shim.Success(resourceAsByte)
}
```

Source : github.com/chainHero/resource-manager/blob/step_1_solved/chaincode/update.go#L114

7

Solve the step 2

Checkout the branch "**step_2**".

There are blanks in the code, in particular it is not possible to acquire a resource for a consumer.

You must replace the TODO in these two files:

- github.com/chainHero/resource-manager/blob/step_2/chaincode/update.go#L42
- github.com/chainHero/resource-manager/blob/step_2/app/fabric/update.go#L58

7

Solutions for the step 2

Checkout the branch "**step_2_solved**" or look at there :

- github.com/chainHero/resource-manager/blob/step_2_solved/app/fabric/update.go
- github.com/chainHero/resource-manager/blob/step_2_solved/chaincode/update.go

7

Solve the `step 3`

Checkout the branch "`step_3`".

There are blanks in the code, in particular it is not possible to release a resource for both a consumer and an admin.

You must change the chaincode and replace the TODO in this file:

github.com/chainHero/resource-manager/blob/step_3/app/web/controllers/release-resource.go#L47

7

Solutions for the `step 3`

Checkout the branch "`step_3_solved`" or look at there :

- github.com/chainHero/resource-manager/blob/step_3_solved/app/fabric/update.go
- github.com/chainHero/resource-manager/blob/step_3_solved/app/web/controllers/release-resource.go
- github.com/chainHero/resource-manager/blob/step_3_solved/chaincode/update.go

Thank you for your attention!

HYPERLEDGER GLOBAL FORUM

https://chainhero.io

CHAINHERO

antoine.chabert@chainhero.io